DOCUMENTO DE SEGURIDAD

PARA EL TRATAMIENTO DE DATOS DE CARACTER PERSONAL

CENVAL, S.L.

DOCUMENTO DE SEGURIDAD

¿Qué es?

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RLOPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD.

ÍNDICE

00 | EXPOSICIÓN DE MOTIVOS

01 | ÁMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD

02 | SISTEMAS DE INFORMACIÓN Y DE LOS RECURSOS PROTEGIDOS

03 | ESTRUCTURA DE LOS FICHEROS Y UBICACIÓN PRINCIPAL DE LOS MISMOS

04 | MEDIDAS DE SEGURIDAD ESTABLECIDAS POR EL REGLAMENTO

05 | REALIZACIÓN DE COPIAS DE RESPALDO Y DE RECUPERACIÓN DE DATOS

06 | FUNCIONES Y OBLIGACIONES DEL PERSONAL

ANEXOS

1. Descripción de los sistemas de información y recursos protegidos.
2. Registro de actividades de tratamiento.
3. Identificación, autenticación, control de acceso y acceso físico.
4. Registro, notificación y respuesta ante incidencias.

4a. Impresos de registro y comunicación de incidencias o brechas de seguridad.

5. Registro de Accesos.
6. Gestión y distribución de soportes.

6a. Registro de salida de soportes.

6b. Registro de entrada de soportes.

7. Controles de verificación.
8. Análisis de riesgos.

8a. Informe del análisis de riesgos.

9. Realización de copias de seguridad y recuperación de datos.
10. Listado de empleados con acceso a datos.
11. Compromiso de confidencialidad empleados.
12. Circular informativa trabajadores.
13. Listado de encargados del tratamiento.
14. Contrato para la regulación del acceso a datos por cuenta de terceros.
15. Consentimiento expreso clientes (pacientes).
16. Consentimiento para el tratamiento de CV.
17. Consentimiento para la publicación de imágenes.
18. Protocolo de actuación a seguir en caso de solicitud de derechos ARCO.

18a. Respuesta cumplimentando el derecho de acceso.

18b. Respuesta a la solicitud de rectificación de datos.

18c. Respuesta a la solicitud de cancelación de datos.

18d. Respuesta a la solicitud de limitación de datos.

18e. Respuesta a la solicitud de portabilidad de datos.

18f. Respuesta a la solicitud de oposición de datos.

18g. Inexistencia de datos personales del interesado en los ficheros de la empresa.

19. Sitio web.

19a. Aviso legal.

19b. Política de privacidad.

19c. Política de cookies.

20. Comunicaciones.

20a. Correo electrónico.

20b. Fax.

20c. Facturas.

0. Exposición de motivos

A través del presente Documento de Seguridad, redactado en cumplimiento de lo dispuesto en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se recogen las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento.

Estas medidas de seguridad afectan a todos los centro de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento automatizado o no automatizado, de los datos de carácter personal contenidos en cualquiera de los ficheros titularidad de Cenval, S.L.

Este documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no automatizados, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

A efectos del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO (Art. 4. Definiciones), se entenderá por:

- Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.
- Autenticación: procedimiento de comprobación de la identidad de un usuario.
- Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
- Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.
- Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
- Ficheros temporales: ficheros de trabajo creados por usuarios o por procesos que son necesarios para el tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
- Identificación: procedimiento de reconocimiento de la identidad de un usuario.
- Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
- Perfil de usuario: accesos autorizados a un grupo de usuarios.
- Recurso: cualquier parte componente de un sistema de información.

- Responsable de seguridad: persona o personas a las que el responsable de fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
- Soporte: objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.
- Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.
- Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

1. Ámbito de aplicación

El presente documento será de aplicación a los tratamientos que contienen datos de carácter personal que se hallan bajo la responsabilidad de Cenval, S.L., incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deben ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

A tal fin, se entiende por dato de carácter personal cualquier información concerniente a personas físicas identificadas o identificables y por sistemas de información el conjunto de tratamientos automatizados o no, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Las medidas de seguridad se clasifican en riesgos (básico, medio, alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

Tratamientos automatizados y no automatizados:

- Riesgo básico:
  Se aplicará a todos los tratamientos con datos de carácter personal y datos de nivel alto.

- Riesgo medio:
  Tratamientos que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, (en estos dos casos, deberán ser de titularidad pública), servicios financieros y prestación de otros servicios de solvencia y crédito).

- Riesgo alto:
  Tratamientos que contengan datos de ideología, afilición sindical, religión, creencias, origen racial, salud o vida sexual o los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas (en este último caso, también deberán ser de titularidad pública), aquellos que contengan datos derivados de actos de violencia de género, y a aquellos que sean responsables los operadores que presten servicios de comunicaciones electrónicas diponibles al público o exploten redes públicas de comunicación electrónica respecto a datos de tráfico y de localización (obligatorio llevar registro de acceso).

2. Descripción de los sistemas de información y los recursos protegidos

La normativa del presente Documento se aplicará a los recursos de los sistemas de información por medio de los cuales se pueden acceder a los tratamientos que contienen datos de carácter personal, así como todo dispositivo que realice procesos de tratamiento, manipulación o almacenamiento de datos de carácter personal.

Del mismo modo se dará suficiente información sobre el tratamiento de los datos de carácter personal. A tal efecto, la Agencia de Protección de datos, define el tratamiento de datos como las operaciones y procedimientos técnicos de carácter automático, manual o mixto, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Los recursos a los que se refiere el mencionado Reglamento son los siguientes:

- Sistema/s operativo/s.
- Nombres de las aplicaciones y/o de los programas destinados al tratamiento de los datos de carácter personal. Diferenciación entre aplicaciones estándares o específicas, dichas aplicaciones deberán incluir en su descripción técnica el nivel de seguridad básico, medio o alto (Disposición adicional única RDLOPD).
- Determinación de los puestos de trabajo.
- Definición del entorno de red.

Los recursos a los que se refiere el párrafo anterior deberán ser detallados en el Anexo 1 del presente documento.

3. Estructura de los tratamientos y ubicación principal de los mismos

El Real Decreto exige determinar la estructura de los ficheros y determinar la ubicación de los mismos.

La Agencia de Protección de Datos, define fichero, como todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Los datos que se han de proporcionar acerca de la estructura y ubicación de cada fichero con datos de carácter personal son:

- Denominación o razón social del responsable del fichero
- Descripción de la actividad principal del responsable del fichero
- N.I.F. / C.I.F.
- Domicilio social
- Localidad, Provincia, Código Postal y País
- Teléfono y Fax
- Correo electrónico
- Nombre del fichero o tratamiento de datos
- Descripción detallada de la finalidad y los usos previstos del mismo
- Tipificación correspondiente a la finalidad y usos previstos
- Origen y procedencia de los datos y colectivos o categorías de interesados
- Tipos de datos, estructura y organización del fichero
- Sistema de tratamiento
- Medidas de seguridad a aplicar

La denominación, estructura y ubicación de los tratamientos con datos de carácter personal quedan recogidos en el Anexo 2.

4. Medidas de seguridad establecidas para alcanzar el nivel exigido por el reglamento

A continuación, se enumeran todas las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por el Reglamento.

Identificación, autenticación y control de acceso

El Real Decreto establece las medidas necesarias para asegurar un acceso restringido a los datos de carácter personal.

El responsable del fichero ha elaborado una relación de los usuarios de dichos datos, que se ha incorporado al presente documento como Anexo 10. A tal efecto, en la citada relación, se especificará el acceso autorizado a cada usuario, que se limitará a los datos y recursos precisos para el desarrollo de sus funciones. La relación se mantendrá actualizada por el responsable de seguridad.

Asimismo, los mecanismos de identificación y autenticación, para el acceso a datos se ven reflejados en el Anexo 3.

Control de acceso físico

Exclusivamente el personal autorizado en este documento de seguridad podrá tener acceso a los sistemas de información con datos de carácter personal y a los locales donde se encuentren los mismos, y en su defecto, estarán bajo respondabilidad de éstos. Los estándares exigidos por la ley para limitar el acceso físico, vienen detallados en el Anexo 3.

Registro de incidencias

Se entiende por incidencia todo hecho o circunstancia que, al producirse, genere cualquier tipo de riesgo o daño que afecte a la seguridad, confidencialidad o integridad de los datos personales contenidos en los ficheros.

El procedimiento de registro, notificación y respuesta ante las incidencias se describe en el Anexo 4.

Registro de accesos

De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

Para garantizar el registro de accesos, el responsable del fichero implantará un sistema de registro de accesos, y delegará en el responsable de seguridad la obligación del control y mantenimiento del mismo.

El procedimiento de registro y las normas aplicables se detallan en el Anexo 5.

Gestión de soportes

Los soportes informáticos, entendiendo por soporte cualquier dispositivo susceptible de contener copias de información extraídas de un recurso informático, que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado.

Las normas, medidas y procedimientos para garantizar que los soportes permitan identificar el tipo de información, así como las condiciones para ser inventariados, almacenados o transportados, se describen en el Anexo 6.

Distribución de soportes

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información sea inteligible y no pueda ser manipulada durante su transporte. Asimismo para poder llevar cabo una distribución, tendrá que dejarse registro detallado de la misma.

Para el cumplimiento de dicha norma, en el Anexo 6, Anexo 6a y Anexo 6b se establecen los procedimientos de cifrado de dichos soportes, así como el registro de los mismos.

Controles de verificación

Para la correcta verificación del cumplimiento de las normas, medidas y procedimientos del presente Documento, y con vistas a detectar cualquier anomalía en los datos de carácter personal o en el tratamiento de los mismos, se han establecido, a cargo del responsable de seguridad los controles periódicos exigidos, que se describen detalladamente en el Anexo 7.

Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

Telecomunicaciones

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. En el caso en que no haya transmisión de datos se hará constar la no transmisión de los mismos.

5. Realización de copias de respaldo y de recuperación de datos

El responsable del fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.

Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

Se conservará una copia de seguridad y de los procedimientos de recuperación de datos en lugar diferente de aquél en que se encuentran los equipos informáticos que los tratan. A esta ubicación se le aplicarán las mismas medidas de seguridad que a la de los Ficheros.

Antes de proceder al almacenamiento de la copia de seguridad se verificará que ésta se ha realizado correctamente y sin ninguna incidencia.

Todo programa o aplicación utilizada para el tratamiento de datos personales deberá proveer la función de realización de copias de seguridad, o bien, permitir la realización de copias de seguridad de tal forma que se garantice la recuperación de datos en los términos expuestos en el presente Documento de Seguridad.

Dichos procedimientos, así como la ejecución de los mismos vienen determinados en el Anexo 9.

6. Funciones y obligaciones del personal

Responsable del tratamiento

Se define, responsable del tratamiento, como la persona física o jurídica que decide sobre la finalidad, contenido y uso de los ficheros de datos personales y de todas aquellas cuestiones que afectan a los mismos, asumiendo, por tanto, la responsabilidad respecto de la correcta aplicación de la normativa concerniente en materia de protección de datos de carácter personal.

El responsable del tratamiento implantará las medidas de seguridad recogidas en el presente Documento, asumiendo la obligación de que todo el personal al que afecte el Documento conozca las obligaciones que le atañen así como las consecuencias en que pudiera incurrir en caso de incumplimiento de las mismas.

A continuación, se enuncian a título indicativo, las funciones del responsable del tratamiento:

- Autorizar, mediante su firma en el impreso de registro de incidencias, la ejecución de los procedimientos de recuperación de datos cuando se hayan visto afectados ficheros cuyo nivel seguridad sea de nivel medio o de nivel alto.

- Conservar los impresos de registro de incidencias que le hayan sido entregados por el responsable de seguridad.

- Comprobar, en colaboración con el responsable de seguridad, la correcta aplicación de los mecanismos de ejecución de copias de seguridad, como de los mecanismos utilizados para la restauración de dichas copias en caso de necesidad

- Autorizar, mediante su firma en el impreso correspondiente, la salida de soportes informáticos que contengan datos de carácter personal, así como la comprobación de la aplicación del cifrado exigido por el Reglamento para la distribución de los mismos.

- Elaborar la relación inicial de usuarios con acceso a sistemas de información que tratan ficheros cuyo contenido sean datos de carácter personal, verificando posteriormente, cualquier modificación que le haya sido propuesta por el responsable de seguridad del fichero, para la actualización de la mencionada relación inicial.

- Conservar los impresos cumplimentados en materia de distribución de soportes, de salidas y entradas de los mismos.

Responsable de seguridad

Dada la posibilidad de la existencia de ficheros cuyo nivel de seguridad haya sido determinado como nivel medio o alto, se cumple la prescripción legal relativa a la designación, por el responsable del fichero, como responsable de seguridad a Don/Doña: Nieves Huertas Cuesta cuya función será la de controlar y coordinar las medidas contenidas en el presente Documento.

En ningún caso esta designación supone una delegación de la responsabilidad ya que esta recaerá en el responsable del fichero.

Independientemente de la obligación genérica en materia de coordinación y control de las medidas de seguridad determinadas en el presente Documento, se relacionan a continuación, a título enunciativo, las funciones específicas del responsable de seguridad:

- Implantar, con la mayor rapidez posible, las medidas necesarias para subsanar cualquier incidencia y entregar al responsable del fichero, los impresos cumplimentados que hayan registrado dicha incidencia.

- En colaboración con el responsable del fichero, comprobará la correcta aplicación tanto de los medios aplicados para la realización de las copias de seguridad, como de los medios utilizados en la recuperación de datos.

- Verificar que, en los procedimientos de recuperación de datos que se hayan realizado por terceros, se mantiene una estricta confidencialidad sobre los datos de carácter personal que contengan los ficheros utilizados para la restauración de los mismos.

- Custodiar, comprobar y actualizar la relación de usuarios y los niveles de acceso a los sistemas de tratamiento de ficheros de carácter personal y a la información contenida en los mismos.

- Asignar a los nuevos usuarios el correspondiente nombre de usuario y una contraseña inicial, dando suficiente información a los mismos de la necesidad de cambiar la contraseña en un plazo no superior a 24 horas, de modo que la contraseña pase a ser de conocimiento exclusivo del usuario.

- Eliminar, en la mayor inmediatez, los identificadores de usuario y contraseña, de los usuarios que sean dados de baja.

- Autorizar la salida o entrada de soportes que contengan datos de carácter personal y determinar la persona designada a tal efecto.

- Realizar la verificación periódica determinada en el Anexo 7.

- Gestionar y controlar el registro de acceso, así como el buen funcionamiento y la no desactivación de los mecanismos designados a tal efecto.

- Implantar y comprobar los estándares y medios necesarios para la correcta ejecución de la normativa sobre datos de carácter personal recogida en el presente Documento.

Resto del personal

Para poder acceder a los ficheros o a los sistemas de información que contengan datos de carácter personal, todo el personal autorizado, está obligado a cumplir la normativa de seguridad contenida en el presente Documento.

El presente Documento de Seguridad es accesible al personal a través de una circular informativa (adjunta en el anexo 12) con los términos que le conciernen a todos los usuarios.

El incumplimiento del presente Documento, así como de cualquiera de las normas contenidas en el mismo, por parte del obligado, podrá considerarse como un quebranto de la buena fe contractual. Se emprenderán acciones legales para la determinación de responsabilidades, si el incumplimiento citado presentase carácter doloso.

Anexo 1 - Descripción de los sistemas de información y de los recursos protegidos

El presente Anexo detalla el conjunto de ficheros, programas, soportes, y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Equipos, impresoras y sistemas operativos instalados

- Nº de Pcs de sobremesa: 30
- Sist. operativo: Windows - Linux
- Nº de Pcs portátiles: 10
- Sist. operativo: Windows - Linux - Mac
- Nº de servidores: 3
- Sist. operativo: Linux
- Nº de impresoras locales: 8
- Nº de impresoras en red: 2

Entorno de red

- Tipo de red: Local - Internet
- Modo de admin. y gestión: sin especificar

Software

- Programas utilizados: Microsoft Office, Libre Office, A3ERP Nomina Cloud

Seguridad

- Sistema copias de seguridad: Servidor interno
- Frecuencia copias de seguridad: diariamente
- Medidas de seguridad implementadas en el local: CIERRE MECÁNICO
- Medidas de seguridad de los ficheros en formato papel: ARCHIVOS BAJO LLAVE

Internet

- Dirección web: www.cenval.es

Anexo 2 - Registro de actividades de tratamiento

Cenval, S.L. con CIF nº B28996551 y domicilio social en C/ Ulises, 104, C.P. 28043 - Madrid (Madrid).

Clientes

Finalidades y usos previstos:

- Gestión de clientes, contable, fiscal y administrativa
- Recursos humanos
- Ejecución de un contrato verbal o escrito
- - Datos Fijos De Los Clientes (nombre, Domicilio, Dni,etc). - Datos Económicos (información Bancaria) - Esta Información Es Utilizada Para Gestionar Los Servicios Prestados A Los Clientes.

Origen y procedencia de los datos:

- El propio interesado o su representante legal

Colectivos o categorías de interesados:

- Clientes y usuarios
- Personas de contacto

Tipos de datos:

- Datos de carácter identificativo:
  - Nombre
  - Apellidos
  - NIF / DNI
  - Dirección
  - Teléfono
  - Correo electrónico

- Datos bancarios:
  - IBAN / Cuenta bancaria

Legitimación mediante:

- Contrato
- Consentimiento

Cantidad de datos:

- Hasta 1000

Cesión de datos:

- No

Transferencia internacional de datos:

- No

Extensión geográfica:

- Ámbito: Nacional

Almacenamiento:

- ¿Cómo se recoge la información personal?
  - Papel
  - Formato electrónico

- ¿A través de qué medios se realiza el tratamiento?
  - Soporte físico
  - Soporte electrónico

- ¿Dónde se almacenan los datos?
  - Sistemas informáticos
  - Archivadores en papel

- Período de almacenamiento:
  - 5 años

Contabilidad

Finalidades y usos previstos:

- - Datos Fijos De Empresas. - Datos Fijos De Clientes Y Proveedores. - Datos Económicos Y Fiscales De Empresas. - Datos Económicos Con Terceros (modelos 347, 349, 180 Y 190). - Datos Fijos De Los Trabajadores (modelo 190).

Origen y procedencia de los datos:

- El propio interesado o su representante legal
- Otras personas físicas
- Entidad privada

Colectivos o categorías de interesados:

- Empleados
- Clientes y usuarios
- Proveedores
- Asociados o miembros

Tipos de datos:

- Datos de carácter identificativo:
  - Nombre
  - Apellidos
  - NIF / DNI
  - Dirección
  - Teléfono
  - Correo electrónico

- Datos bancarios:
  - IBAN / Cuenta bancaria

Legitimación mediante:

- Contrato
- Consentimiento

Cantidad de datos:

- Hasta 1000

Cesión de datos:

- Sí

Transferencia internacional de datos:

- No

Extensión geográfica:

- Ámbito: Nacional

Almacenamiento:

- ¿Cómo se recoge la información personal?
  - Formato electrónico

- ¿A través de qué medios se realiza el tratamiento?
  - Soporte físico
  - Soporte electrónico

- ¿Dónde se almacenan los datos?
  - Sistemas informáticos
  - Archivadores en papel

- Período de almacenamiento:
  - 5 años

Rrhh

Finalidades y usos previstos:

- - Datos Fijos De Los Empleados (nombre, Domicilio, Dni, Etc). - Datos Relativos A Su Situación Personal (historial Laboral, Formación, Etc). - Información Económica (datos Bancarios). - Este Conjunto De Datos Se Utiliza Para La Gestión Empleado Empresa.

Origen y procedencia de los datos:

- El propio interesado o su representante legal
- Otras personas físicas

Colectivos o categorías de interesados:

- Empleados

Tipos de datos:

- Datos de carácter identificativo:
  - Nombre
  - Apellidos
  - NIF / DNI
  - Dirección
  - Teléfono
  - Correo electrónico
  - Imagen
  - Firma

- Características personales:
  - Fecha y lugar de nacimiento
  - Edad
  - Sexo

- Datos académicos:
  - Vida laboral
  - Título

- Datos bancarios:
  - IBAN / Cuenta bancaria

Legitimación mediante:

- Contrato
- Consentimiento

Cantidad de datos:

- Hasta 1000

Cesión de datos:

- Sí

Transferencia internacional de datos:

- No

Extensión geográfica:

- Ámbito: Nacional

Almacenamiento:

- ¿Cómo se recoge la información personal?
  - Papel
  - Formato electrónico

- ¿A través de qué medios se realiza el tratamiento?
  - Soporte físico
  - Soporte electrónico

- ¿Dónde se almacenan los datos?
  - Sistemas informáticos
  - Archivadores en papel

- Período de almacenamiento:
  - 5 años

Proveedores

Finalidades y usos previstos:

- Gestión de clientes, contable, fiscal y administrativa
- Ejecución de un contrato verbal o escrito
- - Datos Fijos De Los Proveedores (nombre, Domicilio, Dni, Etc). - Datos Económicos (información Bancaria). Esta Información Es Utilizada Para Gestionar Los Servicios Prestados A Los Cientes.

Origen y procedencia de los datos:

- El propio interesado o su representante legal
- Entidad privada
- Administraciones Públicas

Colectivos o categorías de interesados:

- Proveedores
- Personas de contacto
- Representante legal

Tipos de datos:

- Datos de carácter identificativo:
  - Nombre
  - Apellidos
  - NIF / DNI
  - Dirección
  - Teléfono
  - Correo electrónico

- Datos bancarios:
  - IBAN / Cuenta bancaria

Legitimación mediante:

- Contrato

Cantidad de datos:

- Hasta 1000

Cesión de datos:

- No

Transferencia internacional de datos:

- No

Extensión geográfica:

- Ámbito: Nacional

Almacenamiento:

- ¿Cómo se recoge la información personal?
  - Papel
  - Formato electrónico

- ¿A través de qué medios se realiza el tratamiento?
  - Soporte físico
  - Soporte electrónico

- ¿Dónde se almacenan los datos?
  - Sistemas informáticos
  - Archivadores en papel

- Período de almacenamiento:
  - 5 años

Cv

Finalidades y usos previstos:

- - Datos Fijos De Los Candidatos (nombre, Domicilio, Dni, Etc). - Datos Personales, Académicos Y Profesionales. - Información Libre Que Se Puede Incluir En Un Cv, Ya Que No Tienen Un Formato Predefinido. - Este Conjunto De Datos Se Utiliza Para La Creación De Una Base De Datos Sobre Posibles Candidatos.

Origen y procedencia de los datos:

- El propio interesado o su representante legal

Colectivos o categorías de interesados:

- Solicitantes

Tipos de datos:

- Datos de carácter identificativo:
  - Nombre
  - Apellidos
  - NIF / DNI
  - Dirección
  - Teléfono
  - Correo electrónico
  - Imagen

- Características personales:
  - Fecha y lugar de nacimiento
  - Edad
  - Sexo

- Datos académicos:
  - Vida laboral
  - Título

Legitimación mediante:

- Consentimiento

Cantidad de datos:

- Hasta 1000

Cesión de datos:

- No

Transferencia internacional de datos:

- No

Extensión geográfica:

- Ámbito: Nacional

Almacenamiento:

- ¿Cómo se recoge la información personal?
  - Papel
  - Formato electrónico

- ¿A través de qué medios se realiza el tratamiento?
  - Soporte físico
  - Soporte electrónico

- ¿Dónde se almacenan los datos?
  - Sistemas informáticos
  - Archivadores en papel

- Período de almacenamiento:
  - 1 año

Videovigilancia

Finalidades y usos previstos:

- Videovigilancia
- - Videovigilancia De Las Instalaciones.

Origen y procedencia de los datos:

- El propio interesado o su representante legal

Colectivos o categorías de interesados:

- Empleados
- Clientes y usuarios
- Proveedores

Tipos de datos:

- Datos de carácter identificativo:
  - Imagen

Cantidad de datos:

- Hasta 1000

Cesión de datos:

- No

Transferencia internacional de datos:

- No

Extensión geográfica:

- Ámbito: Nacional

Almacenamiento:

- ¿Cómo se recoge la información personal?
  - Formato electrónico

- ¿A través de qué medios se realiza el tratamiento?
  - Soporte electrónico

- ¿Dónde se almacenan los datos?
  - Sistemas informáticos

- Período de almacenamiento:
  - 1 mes

Anexo 3 - Identificación, autenticación, control de acceso y acceso físico

Control de acceso

- Los sistemas informáticos que permiten acceso a ficheros que contienen datos de carácter personal tendrán siempre acceso restringido mediante un código de usuario y una contraseña, de modo que la no introducción de dichos requisitos suponga la imposibilidad de acceder a los datos protegidos.
- Se podrá prescindir del código usuario en el caso en que el acceso al sistema informático o a los ficheros de datos se realice exclusivamente por un usuario.
- Los usuarios autorizados (véase Anexo 10), dispondrán de un código de usuario particular asociado a una contraseña que solo conocerá el propio usuario.
- Los registros que se realicen bajo un código de usuario y una contraseña se atribuirán, salvo prueba en contrario, al titular de los mismos y quedarán bajo su responsabilidad personal.
- En el caso, de tratarse de ficheros de nivel medio o alto, se limita la posibilidad de intentar acceder reiteradamente a un máximo de intentos fallidos.

Asignación y cambio de códigos de usuario y contraseñas

- Una vez dado de alta un usuario, el responsable de seguridad confirmará con el responsable del fichero su nivel de acceso a los ficheros que contengan datos de carácter personal. Dicho nivel de acceso sólo podrá modificarse previa consulta con el responsable del fichero y será el estrictamente necesario para el desarrollo de las funciones del usuario.
- El responsable de seguridad asignará a cada usuario el correspondiente código de usuario y una contraseña, la cual será cambiada por el usuario en un plazo no superior a veinticuatro horas, pasando a ser de exclusivo conocimiento por parte del mismo.
- Si un usuario sospecha que su contraseña ha podido ser conocida de manera fortuita o fraudulenta, deberá registrarlo como incidencia, y tendrá que comunicárselo con carácter inmediato al responsable de seguridad, el cual asignará una nueva contraseña al usuario, aplicándose el procedimiento del punto anterior.
- En el caso en que un usuario sea dado de baja, el responsable de seguridad deberá borrar su identificador de usuario sin que, bajo ningún concepto, pueda asignarse a otro usuario.
- Las contraseñas tendrán una longitud mínima de seis caracteres alfanuméricos, y no serán legibles cuando estén siendo tecleadas.

Almacenamiento de contraseñas

- El archivo en el queden almacenadas las contraseñas será accesible exclusivamente por el responsable del fichero o el responsable de seguridad con la autorización expresa de aquél.
- El archivo que recoge las contraseñas mencionadas en el apartado anterior, se almacenará de forma ininteligible.

Acceso y seguridad en los locales donde se encuentran los ficheros

- Sólo el personal autorizado en el Documento de Seguridad puede tener acceso a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal, o en caso de no estar autorizado en el Documento de Seguridad el acceso será supervisado por personal autorizado.
- Descripción de medidas adicionales: CIERRE MECÁNICO

Anexo 4 - Registro, notificación y respuesta ante incidencias

Se ha elaborado el impreso de registro de incidencias (anexo 4a) que obra a disposición de todos los usuarios con acceso a los ficheros, con el fin de que quede debidamente registrada cualquier anomalía o incidencia que al producirse haya puesto en peligro o haya dañado los ficheros de datos:

- Cualquier usuario que tenga conocimiento de una incidencia, se responsabiliza de manera directa y personal del registro de la misma en el mencionado impreso, entregándolo con la mayor inmediatez al responsable de seguridad.

- El responsable de seguridad tomará las medidas oportunas en la mayor brevedad posible, para subsanar las anomalías generadas en las incidencias.

- En el caso en que sea necesario llevar a cabo un proceso de recuperación de datos, será imprescindible que el responsable del fichero autorice la ejecución del procedimiento, haciéndolo constar mediante su firma en el impreso de registro de incidencias.

- El responsable de seguridad tiene la obligación de entregar cumplimentados los impresos de registro de incidencias al responsable del fichero, el cual los conservará numerados correlativamente.

- No registrar una incidencia, o no entregar el impreso cumplimentado al responsable, será considerado como una falta contra la seguridad de los ficheros que podrá constituir quebranto de la buena fe contractual.

Anexo 4a - Impresos de registro de incidencias

Tratamiento objeto de la incidencia: _____

INFORMACIÓN SOBRE LA INCIDENCIA			
Fecha		Hora	
Tipo de incidencia	*(P. Ej.: copia no autorizada de datos, robo de contraseñas, pérdida de soportes, etc.)*		
Descripción detallada de la incidencia	*(Describir la incidencia aportando el mayor nivel de detalle posible.)*		
Efectos que puede producir	*(Detallar los efectos que puede producir la incidencia sobre los datos de carácter personal.)*		
Medidas adoptadas	*(Detallar las medidas adoptadas para eliminar o mitigar los efectos negativos producidos por la incidencia.)*		

INFORMACIÓN SOBRE LA COMUNICACIÓN	
Fecha de notificación	
Persona(s) que realiza(n) la comunicación	

Anexo 5 - Registro de accesos

El presente Anexo recoge el procedimiento de registro de accesos y las normas aplicables correspondientes:

- Se guardará un registro de cada acceso en el que conste la identificación del usuario, la fecha y la hora del acceso, además se registrará el fichero accedido, el tipo de acceso y si fue autorizado y negado en el caso de ficheros y/o datos de nivel alto. Si el acceso se autoriza, se guardará además la información que permita identificar el registro accedido.
- El responsable de seguridad tiene la obligación de controlar directamente los mecanismos establecidos para el registro de accesos, los cuales no podrán ser desactivados en ningún caso.
- El responsable de seguridad revisará periódicamente la información registrada, realizando un informe mensual que certifique la veracidad de los accesos, y las incidencias que se hayan producido en el mismo.
- Los datos registrados se conservarán, como mínimo, durante dos años, para accesos a datos de nivel alto.
- El periodo mínimo de conservación de los datos registrados será de dos años para datos, ficheros y medidas de nivel alto.

Procedimiento empleado para el registro de accesos:

El fichero que realiza y recoge los registros de acceso a datos y ficheros de nivel alto se considera de nivel medio/alto, a su vez dicho fichero se encuentra en formato electrónico encriptado y/o acceso restringido pudiendo existir parte de la información en papel, clasificado en archivos/ficheros bajo llave

El procedimiento para el registro de accesos a dichos ficheros es:

- Identificación del usuario que ha efectuado el acceso.
- Fecha y hora del acceso.
- Tipo de acceso.
- Información necesaria para identificar al registro o registros accedidos.

La desactivación de este fichero tan solo puede efectuarla el administrador del sistema, y autorizado por el responsable de seguridad.

El fichero se guarda un mínimo de dos años después del último acceso o baja del usuario, siendo responsabilidad del administrador del sistema y/o responsable de seguridad, el obtener las copias necesarias y vaciar dicho fichero.

Anexo 6 - Gestión y distribución de soportes

Las medidas enumeradas a continuación se refieren a los soportes que contengan datos personales en cualquier formato, ya sea como copia de seguridad o como resultado de cualquier otro proceso u operación:

- Los soportes estarán claramente identificados con una etiqueta externa que indique qué tipo de información contienen y la fecha de creación de los mismos.
- Los soportes se almacenarán bajo llave, y la utilización de los mismos quedará restringida a las personas con acceso autorizado a los ficheros, según la relación del Anexo 10.
- La salida de soportes fuera de los locales donde están ubicados los ficheros deberá ser expresamente autorizada, mediante sus firmas, por el responsable del fichero y del responsable de seguridad, utilizando para ello el documento de registro de salida adjunto al presente Anexo.
- Se confeccionará un inventario de soportes que contendrá la siguiente información de cada uno de ellos: tipo de soporte, fecha de creación, información que contiene y lugar donde se encuentra almacenado. El inventario tendrá que estar actualizado constantemente.
- En el caso de soportes que vayan a ser desechados, se procederá a su destrucción o inutilización física, previamente a la baja en el inventario, para impedir cualquier recuperación posterior de la información contenida en ellos.
- Los soportes reutilizables deberán ser borrados antes de reutilizarlos de modo que los datos que contenían no sean recuperables.
- Si los soportes tuvieran que salir de los locales en que se encuentren ubicados los ficheros, como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.
- Se establece un sistema de registro de entrada y salida de soportes informáticos mediante la cumplimentación de los correspondientes impresos adjuntos a este Anexo. Este sistema garantiza suficiente conocimiento sobre el tipo de soporte, la fecha y la hora de entrada o salida, el emisor y el destinatario, el número de soportes, el tipo de información alojada en los mismos, la forma de envío, la persona responsable de la entrega y la receptora y la existencia de dicha autorización.
- La recepción de soportes deberá ser autorizada por el responsable de seguridad. Esta autorización podrá efectuarse para cada recepción concreta, mediante la firma del responsable en el impreso de registro, o bien con una autorización genérica por escrito.
- El responsable del fichero conservará los impresos cumplimentados de entradas y salidas de soportes.
- En todo supuesto de distribución de soportes, se cifrarán los datos o bien se utilizará otro mecanismo que garantice que dicha información no sea legible ni se pueda manipular durante su transporte.

Sistema de cifrado para la distribución de soportes:

En la actualidad la distribución de soportes se realiza mediante un cifrado ininteligible. Es un sistema de cifrado que evita que se puedan obtener datos contenidos dentro de los ficheros.

La empresa sólo distribuye recíprocamente datos con sus clientes y sólo los datos relativos a los mismos, nunca datos de terceras personas, y en el caso de haberlos siempre previo consentimiento de los afectados, o por obligación legal en el desarrollo específico de la actividad.

Asimismo la sociedad Cenval, S.L., tal y como establece la ley, utiliza un sistema de cifrado inteligible para la copia de seguridad que posteriormente es almacenada en lugar diferente al que se encuentran los equipos, al menos una de las copias.

Anexo 6a - Registro de salida de soportes

Fecha		Hora	
Tipo de soporte		Nº de soportes	
Emisor		Destinatario	
Forma de envío			
Responsable de la recepción / entrega			
Tipo de información almacenada			

AUTORIZACIÓN DE SALIDA	
Identificación	
Contenido	
Fecha de creación	
Ficheros de donde proceden los datos	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

Anexo 6b - Registro de entrada de soportes

Fecha		Hora	
Tipo de soporte		Nº de soportes	
Emisor		Destinatario	
Forma de envío			
Responsable de la recepción / entrega			
Tipo de información almacenada			

AUTORIZACIÓN DE ENTRADA	
Identificación	
Contenido	
Fecha de creación	
Procedencia de los datos	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

Anexo 7 - Controles de verificación

Las medidas enumeradas a continuación se refieren a los soportes que contengan datos personales en cualquier formato, ya sea como copia de seguridad o como resultado de cualquier otro proceso u operación:

La veracidad y actualización de los datos reflejados en los anexos de este documento, así como el cumplimiento de las normas que contiene, deberán ser periódicamente comprobados de forma que puedan detectarse y subsanarse anomalías, según se determina en los siguientes apartados:

- El responsable de seguridad comprobará, con una periodicidad al menos mensual, los siguientes extremos:
  - Que la lista de usuarios autorizados que se contiene en el Anexo 10 corresponde con la lista de usuarios realmente autorizados en la aplicación de acceso al Fichero, sin que exista ningún nombre de usuario o contraseña vigentes tras la baja del usuario al que pertenecían.
  - La existencia de copias de respaldo que permitan la recuperación de datos.
  - Las incidencias registradas en el libro correspondiente para, independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.
  - La información recogida por el registro de accesos, sobre la cual se elaborará un informe en el que se harán constar todos los datos relevantes y los problemas detectados.

- Los usuarios autorizados comunicarán al responsable de seguridad cualquier cambio del que tengan conocimiento que se produzca respecto a los extremos consignados en los anexos de este documento.

Anexo 8 - Análisis de riesgos

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos establece como requisito esencial que las empresas y profesionales que traten datos personales realicen un Análisis de riesgos.

De tal manera que entendemos por análisis de riesgos, el análisis previo que se debe de dar a todo nuevo tratamiento de datos personales con la principal finalidad de establecer los controles y medidas de seguridad adecuadas para garantizar las libertades y derechos de las personas afectadas.

Apartado 1 del artículo 25 del RGPD:

"Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."

Apartado 2 del artículo 25 del RGPD:

"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento."

Apartado 2 del artículo 32 del RGPD:

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

Anexo 8a - Informe análisis de riesgos

En estos momentos su gestor/a personal le está preparando el informe de análisis de riesgos.

En los próximos días lo tendrá disponible en esta misma página.

Anexo 9 - Realización de copias de seguridad y de recuperación de datos

El reglamento de desarrollo de la LOPD prevé la obligación de conservar una copia de respaldo de los datos de estos ficheros en un lugar diferente del que se encuentran los equipos informáticos que los tratan.

- El responsable del fichero se encargará de verificar, en colaboración con el responsable de seguridad, la correcta aplicación de los procedimientos utilizados para la realización de copias de seguridad y recuperación de datos.

- Los procedimientos de realización de copias de seguridad o recuperaciones de datos garantizarán, en la máxima medida posible, la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la pérdida.

- Se conservará una copia de seguridad y de los procedimientos de recuperación de datos en lugar diferente de aquél en que se encuentran los equipos informáticos que los tratan. A esta ubicación se le aplicarán las mismas medidas de seguridad que a la de los Ficheros.

- Cuando un proceso de recuperación de datos afecte a ficheros de nivel medio o alto, será necesaria la autorización del responsable del fichero para la ejecución del procedimiento de recuperación, en los términos que se han dejado expuestos en la norma 4 del Anexo 4. Asimismo, en ese caso se cumplimentarán los apartados correspondientes del impreso de registro de incidencias.

- Las copias de seguridad se realizarán sobre soporte extraíble y con periodicidad al menos semanal. Este plazo sólo podrá ampliarse en el caso de que en el citado período no se haya producido ninguna actualización o modificación de los datos.

- No obstante, la frecuencia mínima señalada en la norma anterior, no se aplicará excepcionalmente, así, se realizarán copias de seguridad adicionales previamente a la realización de cualquier intervención técnica en los recursos informáticos (por ejemplo: instalación o actualización de aplicaciones, instalación o sustitución de hardware, reparaciones, etc.).

- Antes de proceder al almacenamiento de la copia de seguridad se verificará que ésta se ha realizado correctamente y sin ninguna incidencia. A los soportes donde se contienen las copias de seguridad se les aplicarán las normas relativas a gestión de soportes contenidas en el Anexo 6.

- Todo programa o aplicación utilizada para el tratamiento de datos personales deberá proveer la función de realización de copias de seguridad, o bien, permitir la realización de copias de seguridad de tal forma que se garantice la recuperación de datos en los términos expuestos en las normas precedentes, además dichos programas o aplicaciones deberán incluir en su descripción técnica el nivel de seguridad.

- Todo procedimiento de recuperación de datos deberá ser realizado por personal con los necesarios conocimientos técnicos. En el caso de que dicho procedimiento sea realizado por personal externo, el responsable de seguridad verificará que durante su ejecución se mantenga la más estricta confidencialidad sobre los datos de carácter personal obrantes en los ficheros.

- **Procedimiento utilizado para la realización de copias de seguridad:**

Servidor interno

Anexo 10 - Listado de empleados con acceso a datos

Mediante el presente anexo se detalla el nivel de acceso a ficheros con datos de carácter personal por parte de usuarios de: Cenval, S.L..

NIVEL DE ACCESO AUTORIZADO A DATOS:

- Total: El usuario tiene acceso a todos los recursos. Tiene permisos de lectura y de escritura en todos los recursos de la red.
- Usuario: El usuario tiene acceso de lectura y escritura a los recursos propios necesarios para el desarrollo de su actividad.
- Consulta: El usuario sólo tiene acceso de lectura a ciertos recursos.

REGISTRO DE USUARIOS:

Anexo 11 - Compromiso de confidencialidad empleados

En Madrid, a 10 de Mayo del 2021

De acuerdo al Reglamento General de Protección de Datos relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), de conformidad con la Ley de Competencia Desleal 3/1991, incluyendo su modificación a través de la Ley 29/2009, y de la Ley Orgánica 5/2010 por la que se modifica el Código Penal de 1995, le informamos que:

Responsable del tratamiento:

Sus datos pasarán a formar parte de un fichero titularidad de Cenval, S.L., con domicilio social en:
C/ Ulises, 104, con NIF nº B28996551 y registrado en Madrid (Madrid).

Finalidad: Las finalidades del tratamiento de sus datos serán las siguientes:

- Recursos Humanos:
  Tienen como finalidad desarrollar, mantener, cumplir y controlar su actividad, para dar cumplimiento a las obligaciones y funciones del departamento de Recursos Humanos relativas a las actividades de formación, control de asistencia al trabajo, formalización de las nóminas, deberes en materia de prevención de riesgos laborales, así como la gestión de canales de comunicación/denuncias implementados por la entidad de conformidad con requisitos previstos en las normativas en materia de cumplimiento vigentes.

- Derechos de imagen:
  Tienen como finalidad la utilización de su imagen para la elaboración de publicaciones internas y para su utilización con finalidades de marketing y prospección comercial de la entidad, así como a la publicación de su CV e información de su trayectoria profesional en nuestra intranet, webs y blogs corporativos. En ningún caso estas imágenes e información de carácter personal serán cedidas a terceros, ni utilizadas para una finalidad distinta a la descrita.

- Control y registro de jornada:
  Control de accesos al centro de trabajo, así como de las horas de entrada y salida del trabajador, en virtud de la obligación del empleador de registrar dicha información del empleado.

Legitimación:

La legitimación para la recogida de sus datos se basa en el contrato suscrito con Cenval, S.L..

Destinarios:

De igual modo, le informamos que para el cumplimiento de las obligaciones legales y laborales sus datos pueden ser comunicados a:

- Administraciones Públicas (Seguridad Social, Agencia Tributaria, Subvenciones).
- Mutuas de protección laboral y servicios de prevención de riesgos laborales o la preservación de la salud de los trabajadores.
- Aquellas entidades o clientes que exijan o ante las cuales sea necesario identificar a los empleados: entidades bancarias para pagos de nóminas, aseguradoras, proyectos, formación, mensajería, renting, identificación de infracciones de tráfico, así como aquellas entidades o clientes que requieran datos identificativos y laborales del personal para llevar a cabo el servicio contratado y que acrediten la relación con la empresa.
- Comités de empresa, sindicatos y delegados de prevención.

Sus datos no serán cedidos para otras finalidades distintas a las anteriormente descritas.

Derechos:

Puede ejercer sus derechos de acceso, rectificación, supresión y oposición, así como revocar su autorización para el uso de sus imágenes.

También podrá solicitar la limitación u oposición al tratamiento de sus datos cuando se den determinadas circunstancias, en cuyo caso únicamente serán conservados para el cumplimiento de las obligaciones legalmente previstas.

Para ejercer los derechos anteriormente descritos deberá dirigirse a Cenval, S.L.. De igual modo, le informamos de que la Agencia Española de Protección de Datos es el órgano competente destinado a la tutela de estos derechos.

Con la finalidad de mantener actualizados los datos, usted deberá comunicar cualquier cambio que se produzca sobre los mismos.

Compromiso de confidencialidad:

En atención a nuestro más alto compromiso de cumplir con la legalidad vigente, le informamos que bajo ningún concepto usted debe utilizar ni incorporar a los sistemas informáticos y archivos documentales de esta Entidad la información de carácter personal o empresarial a la que haya tenido acceso durante el desempeño de sus tareas o funciones en otras entidades, cuando ello pueda implicar la vulneración de las legislaciones anteriormente mencionadas.

En cumplimiento de la legislación anteriormente mencionada, usted asume el compromiso de guardar secreto profesional respecto de los datos personales, datos sobre los clientes, estrategias comerciales y organizativas e industriales, y cualquier otra información a la que tenga acceso con el motivo de las funciones asignadas. Dicha obligación de secreto profesional subsistirá en cumplimiento del artículo 32 del RGPD, aun después de finalizar la relación laboral.

De igual modo, le informamos que con la finalidad de garantizar el derecho a la intimidad y privacidad del trabajador por parte de Cenval, S.L., bajo ningún concepto usted debe incorporar a los sistemas informáticos y archivos documentales de esta entidad, su información de carácter personal tales como fotos, videos o imágenes.

Asimismo, de conformidad con el mismo artículo 32 del RGPD, el empleado se compromete a cumplir las normas internas de seguridad que afectan al desarrollo de sus funciones, así como el uso de los equipos informáticos, correo electrónico y demás aplicaciones a las que va a tener acceso. De igual modo, el empleado, como parte necesaria y fundamental para conseguir el compromiso de responsabilidad corporativa y ética empresarial de esta Entidad, tiene la responsabilidad y el deber de realizar los programas formativos y aplicar los procedimientos y normas que se le comuniquen a tal efecto.

Por último, en virtud de las nuevas implicaciones para la empresa como consecuencia de la entrada en vigor de la Reforma del Código Penal del año 2010 y las aclaraciones y nuevos requisitos establecidos en la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal, en relación a las nuevas implicaciones y responsabilidades en materia de Responsabilidad Penal de la Empresa (RPE), el empleado se compromete a aplicar y tener en consideración los protocolos y procedimientos que establezca la entidad en esta materia y que sean de aplicación en el ámbito de protección de datos de carácter personal en los términos previstos en este documento.

Ante cualquier duda, incidente, o imposibilidad de aplicación adecuada de los procedimientos y normas lo comunicará al responsable que se le designe en cada uno de los supuestos tal como quede establecido a tal efecto.

Don/Doña: _____

(Nombre y apellidos del empleado/a)

_____

Anexo 12 - Circular informativa para los trabajadores

La presente circular tiene como objetivo básico la difusión de las funciones y obligaciones del personal de Cenval, S.L. en materia de seguridad de datos personales.

La protección se basa en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Estas normas protegen y garantizan las libertades y los derechos fundamentales de las personas físicas y especialmente su honor e intimidad. Con este fin se contemplan multas por parte de la Agencia de Protección de Datos de hasta 601.012,10€ en función de la calificación de la infracción cometida.

El citado RGPD tiene como objetivo primordial, entre otros, implementar las medidas de índole técnicas y organizativas necesarias para garantizar la seguridad que deben reunir tanto ficheros automatizados como en papel, los centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento de los datos de carácter personal.

Para recoger todas las medidas definidas anteriormente y garantizar con lo dispuesto en el Reglamento de Seguridad, Cenval, S.L. ha elaborado un Documento de Seguridad y ha nombrado Responsable de Seguridad a Nieves Huertas Cuesta. Estas medidas de seguridad son de obligado cumplimiento por todo el personal de la empresa con acceso a datos de carácter personal.

El citado Documento de Seguridad se encuentra a disposición de todo trabajador, previa solicitud al Responsable de Seguridad.

A continuación se presenta un resumen de los aspectos más relevantes:

- Recursos del sistema de información: Queda terminantemente prohibido utilizar dichos recursos a los que se tenga acceso para uso privado o para cualquier otra finalidad diferente de la del desempeño de sus funciones. Bajo ningún concepto puede revelarse información a persona alguna ajena a la empresa, sin la debida autorización.

- Los sistemas informáticos que dan acceso a los ficheros que contienen datos de carácter personal tendrán siempre este acceso restringido mediante un código de usuario y una contraseña, sin cuya introducción resulte imposible acceder a los datos protegidos.

- El código de usuario y la contraseña son absolutamente personales e intransferibles; por ello, los registros que se efectúen sobre operaciones realizadas bajo un código y contraseña se atribuirán, salvo prueba en contrario, al titular de los mismos y quedarán bajo su responsabilidad personal.

- Cada usuario es responsable de la confidencialidad de su contraseña, por lo que si advierte o sospecha que la misma ha podido ser conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y notificárselo de inmediato al Responsable de Seguridad, el cual asignará una nueva contraseña al usuario.

- Salidas de soportes: Toda salida de cualquier soporte y/o ordenador personal fuera de la organización deberá ser expresamente autorizada según el procedimiento descrito en el Documento de seguridad.

- Incidencias en materia de seguridad: El usuario que tenga conocimiento de la incidencia se responsabiliza directa y personalmente de comunicarla según las instrucciones determinadas en el Documento de Seguridad.

- Compromiso: Todos los compromisos anteriores deben mantenerse, incluso después de extinguida por cualquier causa la relación laboral con la empresa.

- Responsabilidad: El incumplimiento por el obligado, de cualquiera de las normas contenidas en el presente documento y, por ende, en el Documento de Seguridad podrá considerarse como un quebranto de la buena fe contractual. Si el incumplimiento tuviera carácter doloso, se emprenderán las acciones legales correspondientes para la debida depuración de responsabilidades.

Cualquier duda o comentario que pudiese suscitar el presente documento puede ser consultada o atendida por el Responsable de Seguridad.

En _____, a ___ de _____ de 20___

_____

(Trabajador/a)

Anexo 13 - Listado de encargados del tratamiento

Grupo Ático34, S.L.

- B-87186177
- Paseo de la Castellana 95, 15
- C.P. 28046 - Madrid
- madrid@atico34.com
- 91 489 64 19

- Responsable: Javier Oviaño Pérez
- NIF: 72742529-S

- Servicio: Consultoría en materia de protección de datos.

- Duración del servicio: Mientras dure la prestación del servicio acordado por las partes.

- ¿Accede a datos?: Sí

- ¿Subcontratación permitida?: No

- ¿Notificación violación por encargado?: No

- Destino final de los datos: Encargado

Tratamientos relacionados:

- Empleados
- Proveedores

Servicio Prevención

-
-
-
-
-
-
-
- Responsable:
- NIF:

- Servicio: Servicio De Prevención De Riesgos

- Duración del servicio: Mientras Dure La Prestación

- ¿Accede a datos?: Sí

- ¿Subcontratación permitida?: No

- ¿Notificación violación por encargado?: No

- Destino final de los datos: Responsable

Tratamientos relacionados:

- Clientes
- Contabilidad
- Rrhh
- Proveedores

Anexo 14 - Contrato para la regulación del acceso a datos por cuenta de terceros

En Madrid, a 10 de Mayo del 2021

REUNIDOS:

De una parte, Don/Doña Sara Macho Marques, provisto de NIF nº: 02639045W, actuando como representante legal de Cenval, S.L., con domicilio en: C/ Ulises, 104, C.P. 28043 - Madrid (Madrid) y NIF nº: B28996551, en adelante RESPONSABLE DEL TRATAMIENTO.

De otra parte, Don Javier Oviaño Pérez, provisto de NIF nº: 72742529-S, actuando como legal representante de Grupo Ático34, S.L., con domicilio en: Paseo de la Castellana 95, 15, 28046 - Madrid y NIF nº: B-87186177, en adelante el ENCARGADO DEL TRATAMIENTO.

Ambas partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato de encargo de tratamiento de datos personales y para quedar obligadas en la representación en que respectivamente actúan, en los términos convenidos en él. A tal fin,

MANIFIESTAN:

1º - Que ambas partes se encuentran vinculadas por una relación contractual de carácter mercantil para la prestación de un servicio de consultoría en materia de protección de datos (en adelante SERVICIO).

2º - Que para la prestación de dicho servicio es necesario que el ENCARGADO DEL TRATAMIENTO tenga acceso a datos de carácter personal de los siguientes tratamientos relacionados:

- **Empleados**
- **Proveedores**

Estos tratamientos son responsabilidad del RESPONSABLE DEL FICHERO, por lo que asume las funciones y obligaciones que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, estipula para los Encargados de Tratamiento.

3º - Ambas partes reconocen cumplir con todas las obligaciones derivadas de la normativa comunitaria y nacional en materia de protección de datos, en especial las relativas al derecho de información, consentimiento y deber de secreto, así como a la adopción de las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos personales.

4º - Que, en cumplimiento del artículo 28 del RGPD, ambas partes de forma libre y espontánea voluntad, acuerdan regular este acceso y tratamiento de datos de carácter personal de conformidad con las siguientes:

ESTIPULACIONES:

PRIMERO: OBJETO DEL CONTRATO

Mediante las presentes cláusulas se habilita a la entidad ENCARGADA DE TRATAMIENTO, para tratar por cuenta del, RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal necesarios para prestar el servicio anteriormente descrito.

SEGUNDO: IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE DEL TRATAMIENTO, pone a disposición del ENCARGADO DEL TRATAMIENTO, la información que se describe a continuación:

- _____
- _____

TERCERO: DURACIÓN

El presente acuerdo estará en vigor mientras dure la prestación del servicio acordado por las partes.

Una vez finalice el presente contrato, el ENCARGADO DE TRATAMIENTO deberá devolver al RESPONSABLE o a otro encargado que designe el RESPONSABLE los datos personales y suprimir cualquier copia que obre en su poder.

CUARTO: OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO

El ENCARGADO DEL TRATAMIENTO y todo su personal se obliga a:

1. 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.

2. 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 Reglamento (UE) 2016/679 o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

3. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga*:

** NOTA: Las obligaciones indicadas en este apartado, no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del Reglamento (UE) 2016/679, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.*

A) 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.

B) Las categorías de tratamientos efectuados por cuenta de cada responsable.

C) En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del Reglamento (UE) 2016/679 , la documentación de garantías adecuadas.

D) Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

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

4. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

5. Subcontratación.

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del ENCARGADO. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 72 horas, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido. El subcontratista, que también tendrá la condición de ENCARGADO DEL TRATAMIENTO, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO DEL TRATAMIENTO y las instrucciones que dicte el responsable.

Corresponde al ENCARGADO inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

6. El ENCARGADO DEL TRATAMIENTO deberá observar en todo momento, y en relación con los ficheros de datos de carácter personal a los que tuviera acceso o le pudieren ser entregados por el Responsable, para la realización en cada caso de los trabajos y servicios que pudieren acordarse, el deber de confidencialidad y secreto profesional que, de conformidad con lo dispuesto en la normativa de Protección de Datos, subsistirá aun después de finalizar la relación de los trabajos encargados en relación con cualquier fichero así como, en su caso, tras la finalización por cualquier causa del presente contrato.

7. 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.*

** NOTA: Si existe una obligación de confidencialidad de naturaleza estatutaria o legal (por ejemplo, abogados) deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.*

8. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

9. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

10. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

- Acceso, rectificación, supresión y oposición.
- Limitación del tratamiento.
- Portabilidad de datos.
- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

El ENCARGADO DEL TRATAMIENTO debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.

11. Derecho de información

El RESPONSABLE DEL TRATAMIENTO, debe facilitar a los interesados, la información relativa a los tratamientos de sus datos que se van a realizar.

12. Notificación de violaciones de la seguridad de los datos

El ENCARGADO DEL TRATAMIENTO notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, y a través de correo electrónico con confirmación de lectura, 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. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- 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.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- 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.

** NOTA: Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.*

- Corresponde al RESPONSABLE DEL TRATAMIENTO comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

  La comunicación contendrá, como mínimo, la información siguiente:

- 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.
- Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- 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.

13. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

14. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las consultas previas a la autoridad de control, cuando proceda.

15. 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.

16. Implantar las siguientes medidas de seguridad:

Todas aquellas necesarias para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.

17. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

18. Destino final de los datos:

Devolver al ENCARGADO que designe por escrito el RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida 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.

QUINTO: OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Corresponde al RESPONSABLE DEL TRATAMIENTO:

1. Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
2. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
3. Realizar las consultas previas que corresponda.
4. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento (UE) 2016/679 por parte del encargado.
5. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

SEXTO: RESPONSABILIDAD DEL ENCARGADO DE TRATAMIENTO

1. El ENCARGADO DEL TRATAMIENTO será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el ENCARGADO DEL TRATAMIENTO responderá de las infracciones en que hubiera incurrido personalmente.

2. El ENCARGADO DEL TRATAMIENTO indemnizará al RESPONSABLE DEL TRATAMIENTO por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.

3. A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El ENCARGADO DEL TRATAMIENTO, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.

4. La responsabilidad del ENCARGADO DEL TRATAMIENTO incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el RESPONSABLE DEL TRATAMIENTO, como resultado del incumplimiento del ENCARGADO DEL TRATAMIENTO de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del RESPONSABLE DEL TRATAMIENTO en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

SÉPTIMO: CONTROLES Y AUDITORÍA

El RESPONSABLE DEL TRATAMIENTO, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del ENCARGADO DEL TRATAMIENTO del presente contrato.

Por su parte, el Encargado deberá facilitar al RESPONSABLE DEL TRATAMIENTO cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

OCHO: NOTIFICACIONES

1. Cualquier notificación que se efectúe entre las partes se hará por escrito y será entregada personalmente o de cualquier otra forma que certifique la recepción por la parte notificada.

2. Cualquier cambio de domicilio de una de las partes deberá ser notificado a la otra de forma inmediata y por un medio que garantice la recepción del mensaje.

NUEVE: CLÁUSULAS GENERALES

1. La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituye una renuncia a dichos derechos en el futuro.
2. La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.
3. Si se llegara a demostrar que alguna de las estipulaciones contenidas en este Contrato es nula, ilegal o inexigible, la validez, legalidad y exigibilidad del resto de las estipulaciones no se verán afectadas o perjudicadas por aquélla.
4. El presente Contrato y las relaciones entre el RESPONSABLE DEL TRATAMIENTO y el ENCARGADO DEL TRATAMIENTO no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.
5. Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

D./Dª. Sara Macho Marques

D./Dª. Javier Oviaño Pérez

_____

(En nombre del RESPONSABLE)

_____

(En nombre del ENCARGADO)

En Madrid, a 10 de Mayo del 2021

REUNIDOS:

De una parte, Don/Doña Sara Macho Marques, provisto de NIF nº: 02639045W, actuando como representante legal de Cenval, S.L., con domicilio en: C/ Ulises, 104, C.P. 28043 - Madrid (Madrid) y NIF nº: B28996551, en adelante RESPONSABLE DEL TRATAMIENTO.

De otra parte, Don/Doña _____, provisto de NIF nº: _____, actuando como legal representante de Servicio Prevención, con domicilio en: , C.P. - () y NIF nº: , en adelante el ENCARGADO DEL TRATAMIENTO.

Ambas partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato de encargo de tratamiento de datos personales y para quedar obligadas en la representación en que respectivamente actúan, en los términos convenidos en él. A tal fin,

MANIFIESTAN:

1º - Que ambas partes se encuentran vinculadas por una relación contractual de carácter mercantil para la prestación de Servicio De Prevención De Riesgos (en adelante SERVICIO).

2º - Que para la prestación de dicho servicio es necesario que el ENCARGADO DEL TRATAMIENTO tenga acceso a datos de carácter personal de los siguientes tratamientos relacionados:

- **Rrhh**

Estos tratamientos son responsabilidad del RESPONSABLE DEL FICHERO, por lo que asume las funciones y obligaciones que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, estipula para los Encargados de Tratamiento.

3º - Ambas partes reconocen cumplir con todas las obligaciones derivadas de la normativa comunitaria y nacional en materia de protección de datos, en especial las relativas al derecho de información, consentimiento y deber de secreto, así como a la adopción de las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos personales.

4º - Que, en cumplimiento del artículo 28 del RGPD, ambas partes de forma libre y espontánea voluntad, acuerdan regular este acceso y tratamiento de datos de carácter personal de conformidad con las siguientes:

ESTIPULACIONES:

PRIMERO: OBJETO DEL CONTRATO

Mediante las presentes cláusulas se habilita a la entidad ENCARGADA DE TRATAMIENTO, para tratar por cuenta del, RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal necesarios para prestar el servicio anteriormente descrito.

SEGUNDO: IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE DEL TRATAMIENTO, pone a disposición del ENCARGADO DEL TRATAMIENTO, la información que se describe a continuación:

- _____
- _____

TERCERO: DURACIÓN

El presente acuerdo tiene una duración de Mientras Dure La Prestación.

Una vez finalice el presente contrato, el ENCARGADO DE TRATAMIENTO debe suprimir/devolver al RESPONSABLE, o devolver a otro encargado que designe el RESPONSABLE los datos personales y suprimir cualquier copia que esté en su poder.

CUARTO: OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO

El ENCARGADO DEL TRATAMIENTO y todo su personal se obliga a:

1. 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.

2. 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 Reglamento (UE) 2016/679 o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

3. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga*:

** NOTA: Las obligaciones indicadas en este apartado, no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del Reglamento (UE) 2016/679, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.*

A) 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.

B) Las categorías de tratamientos efectuados por cuenta de cada responsable.

C) En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del Reglamento (UE) 2016/679 , la documentación de garantías adecuadas.

D) Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

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

4. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

5. Subcontratación.

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del ENCARGADO. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 72 horas, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido. El subcontratista, que también tendrá la condición de ENCARGADO DEL TRATAMIENTO, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO DEL TRATAMIENTO y las instrucciones que dicte el responsable.

Corresponde al ENCARGADO inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

6. El ENCARGADO DEL TRATAMIENTO deberá observar en todo momento, y en relación con los ficheros de datos de carácter personal a los que tuviera acceso o le pudieren ser entregados por el Responsable, para la realización en cada caso de los trabajos y servicios que pudieren acordarse, el deber de confidencialidad y secreto profesional que, de conformidad con lo dispuesto en la normativa de Protección de Datos, subsistirá aun después de finalizar la relación de los trabajos encargados en relación con cualquier fichero así como, en su caso, tras la finalización por cualquier causa del presente contrato.

7. 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.*

** NOTA: Si existe una obligación de confidencialidad de naturaleza estatutaria o legal (por ejemplo, abogados) deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.*

8. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

9. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

10. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

- Acceso, rectificación, supresión y oposición.
- Limitación del tratamiento.
- Portabilidad de datos.
- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

El ENCARGADO DEL TRATAMIENTO debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.

11. Derecho de información

El RESPONSABLE DEL TRATAMIENTO, debe facilitar a los interesados, la información relativa a los tratamientos de sus datos que se van a realizar.

12. Notificación de violaciones de la seguridad de los datos

El ENCARGADO DEL TRATAMIENTO notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, y a través de correo electrónico con confirmación de lectura, 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. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- 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.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- 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.

** NOTA: Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.*

- Corresponde al RESPONSABLE DEL TRATAMIENTO comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

  La comunicación contendrá, como mínimo, la información siguiente:

- 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.
- Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- 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.

13. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

14. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las consultas previas a la autoridad de control, cuando proceda.

15. 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.

16. Implantar las siguientes medidas de seguridad:

Todas aquellas necesarias para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.

17. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

18. Destino final 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 comporta 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.

QUINTO: OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Corresponde al RESPONSABLE DEL TRATAMIENTO:

1. Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
2. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
3. Realizar las consultas previas que corresponda.
4. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento (UE) 2016/679 por parte del encargado.
5. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

SEXTO: RESPONSABILIDAD DEL ENCARGADO DE TRATAMIENTO

1. El ENCARGADO DEL TRATAMIENTO será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el ENCARGADO DEL TRATAMIENTO responderá de las infracciones en que hubiera incurrido personalmente.

2. El ENCARGADO DEL TRATAMIENTO indemnizará al RESPONSABLE DEL TRATAMIENTO por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.

3. A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El ENCARGADO DEL TRATAMIENTO, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.

4. La responsabilidad del ENCARGADO DEL TRATAMIENTO incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el RESPONSABLE DEL TRATAMIENTO, como resultado del incumplimiento del ENCARGADO DEL TRATAMIENTO de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del RESPONSABLE DEL TRATAMIENTO en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

SÉPTIMO: CONTROLES Y AUDITORÍA

El RESPONSABLE DEL TRATAMIENTO, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del ENCARGADO DEL TRATAMIENTO del presente contrato.

Por su parte, el Encargado deberá facilitar al RESPONSABLE DEL TRATAMIENTO cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

OCHO: NOTIFICACIONES

1. Cualquier notificación que se efectúe entre las partes se hará por escrito y será entregada personalmente o de cualquier otra forma que certifique la recepción por la parte notificada.

2. Cualquier cambio de domicilio de una de las partes deberá ser notificado a la otra de forma inmediata y por un medio que garantice la recepción del mensaje.

NUEVE: CLÁUSULAS GENERALES

1. La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituye una renuncia a dichos derechos en el futuro.
2. La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.
3. Si se llegara a demostrar que alguna de las estipulaciones contenidas en este Contrato es nula, ilegal o inexigible, la validez, legalidad y exigibilidad del resto de las estipulaciones no se verán afectadas o perjudicadas por aquélla.
4. El presente Contrato y las relaciones entre el RESPONSABLE DEL TRATAMIENTO y el ENCARGADO DEL TRATAMIENTO no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.
5. Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

D./Dª. Sara Macho Marques

D./Dª. _____

_____

(En nombre del RESPONSABLE)

_____

(En nombre del ENCARGADO)

Anexo 15 - Consentimiento expreso clientes

En aras a dar cumplimiento al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y siguiendo las Recomendaciones e Instrucciones emitidas por la Agencia Española de Protección de Datos (A.E.P.D.), SE INFORMA:

- Los datos de carácter personal solicitados y facilitados por usted, son incorporados a un fichero de titularidad privada cuyo responsable y único destinatario es Cenval, S.L..
- Solo serán solicitados aquellos datos estrictamente necesarios para prestar adecuadamente el servicio, pudiendo ser necesario recoger datos de contacto de terceros, tales como representantes legales, tutores, o personas a cargo designadas por los mismos.
- Todos los datos recogidos cuentan con el compromiso de confidencialidad exigido por la normativa, con las medidas de seguridad establecidas legalmente, y bajo ningún concepto son cedidos o tratados por terceras personas, físicas o jurídicas, sin el previo consentimiento del cliente, tutor o representante legal, salvo en aquellos casos en los que fuere imprescindible para la correcta prestación del servicio.
- Una vez finalizada la relación entre la empresa y el cliente los datos serán archivados y conservados, durante un periodo tiempo mínimo de _____, tras lo cual seguirá archivado o en su defecto serán devueltos íntegramente al cliente o autorizado legal.

☐ He sido informado de que los datos que facilito serán incluidos en el Fichero denominado Clientes de Cenval, S.L., con la finalidad de gestión del tratamiento asignado, emisión de facturas, contacto..., a lo cual manifiesto mi consentimiento. También se me ha informado de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación, oposición, limitación y portabilidad indicándolo por escrito a Cenval, S.L. con domicilio en: C/ Ulises, 104, C.P. 28043 - Madrid (Madrid).

☐ Consiento que mis datos personales sean cedidos por Cenval, S.L. a las entidades que prestan servicios a la misma.

☐ ACEPTO que Cenval, S.L. me remita comunicaciones informativas a través de e-mail, SMS, o sistemas de mensajería instantánea como Whatsapp, con el objetivo de mantenerme informado/a del desarrollo de las actividades propias del servicio contratado.

☐ ACEPTO Y SOLICITO EXPRESAMENTE, la recepción de comunicaciones comerciales por vía electrónica (e-mail, Whatsapp, bluetooth, SMS), por parte de Cenval, S.L., sobre productos, servicios, promociones y ofertas de mi interés.

Nombre y apellidos: _____ DNI: _____
(Cliente)

Representante legal: _____ DNI: _____
(Menores de edad)

En _____, a ___ de _____ de 20___

_____

Anexo 16 - Consentimiento para el tratamiento y cesión de CV

Cenval, S.L., con CIF/NIF nº: B28996551, le informa que conforme dispone el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo referente al tratamiento de datos personales y a la libre circulación de estos, que los datos personales facilitados y recogidos en esta solicitud de empleo o currículum vitae, serán tratados e incluidos automatizadamente en los ficheros de datos personales bajo responsabilidad de Cenval, S.L., donde se recogen y almacenan los datos personales con la finalidad exclusiva de formar parte en los procesos de selección de personal, bolsa de trabajo y contratación que se lleven a cabo.

El interesado otorga su consentimiento para el tratamiento de sus datos personales con la finalidad anteriormente mencionada. En el supuesto de producirse alguna modificación de sus datos personales, le solicitamos, nos lo comunique por escrito con la única finalidad de mantener actualizada su solicitud de empleo o currículum vitae.

☐ El titular de los datos personales consiente expresa e inequívocamente a que sus datos personales se cedan a otras organizaciones interesadas en determinados perfiles de trabajo.

Cenval, S.L., garantiza el buen uso de la información, y en especial, la plena confidencialidad de los datos de carácter personal contenidos en nuestros ficheros, así como el pleno cumplimiento de las obligaciones en materia de protección de datos de carácter personal.

De acuerdo con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo referente al tratamiento de datos personales y a la libre circulación de estos, Cenval, S.L., se compromete a respetar su confidencialidad en el tratamiento de sus datos personales, y le informa que tiene derecho a ejercitar los derechos de acceso, rectificación, cancelación, oposición, limitación y portabilidad de sus datos personales mediante solicitud escrita, adjuntando fotocopia del D.N.I., dirigida a Cenval, S.L., con domicilio en: C/ Ulises, 104, C.P. 28043 - Madrid (Madrid).

Don/Doña: _____ DNI: _____

(Nombre y apellidos del solicitante)

En _____, a ___ de _____ de 20___

_____

Anexo 17 - Consentimiento para la publicación de imágenes

Cenval, S.L.

Con la inclusión de las nuevas tecnologías dentro de las comunicaciones, publicaciones y acciones comerciales que puede realizar Cenval, S.L. y la posibilidad de que en estas puedan aparecer los datos personales y/o imágenes que ha proporcionado a nuestra empresa dentro del vínculo comercial existente;

Y dado que el derecho a la propia imagen está reconocido en el artículo 18 de la Constitución y regulado por la Ley 1/1982, de 5 de mayo, sobre el derecho al honor, a la intimidad personal y familiar y a la propia imagen y el Reglamento General de Protección de Datos relativo a la protección de las personas físicas en lo referente al tratamiento de datos personales y a la libre circulación de estos datos (RGPD),

Cenval, S.L., pide el consentimiento a los clientes para poder publicar las imágenes en las cuales aparezcan individualmente o en grupo que con carácter comercial se puedan realizar a los clientes, en las diferentes secuencias y actividades realizadas -en nuestras instalaciones y fuera de las mismas- en actividades contratadas con nuestra empresa.

Don / Doña: _____, con DNI nº _____, autorizo a Cenval, S.L. a un uso de las imágenes realizadas en servicios contratados con vuestra empresa y publicadas en:

- La página web y perfiles en redes sociales de la empresa.
- Filmaciones destinadas a la difusión comercial.
- Fotografías para revistas y/o publicaciones de ámbito relacionado con el sector.

En _____, a ___ de _____ de 20___

_____

(El cliente / La clienta)

Anexo 18. Protocolo de actuación a seguir en caso de solicitud de derechos ARCO

La Ley de Protección de Datos de Carácter Personal otorga a los particulares cuyos datos obren en ficheros automatizados cinco derechos básicos respecto a los mismos:

- Derecho de información
- Derecho de acceso
- Derecho de rectificación
- Derecho de cancelación
- Derecho de limitación
- Derecho a la portabilidad
- Derecho de oposición

En cumplimiento de las disposiciones legales vigentes, se ofrecerá a las personas a las que se les recaban datos personales la posibilidad de ejercitar tales derechos dirigiéndose por escrito al responsable del fichero.

A continuación se exponen los protocolos de actuación a seguir para la correcta cumplimentación de tales solicitudes.

Derecho de información:

El derecho de información previo al tratamiento de los datos de carácter personal es uno de los derechos básicos y principales contenidos en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO; por tanto, si se van a registrar y tratar datos de carácter personal será necesario informar a los interesados, a través del medio que se utilice para la recogida, del contenido de los Art.12, 13 y 14 que regulan el derecho de información a los afectados previo a la recogida de los datos:

- Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, precio e inequívoco:

  - De la existencia de un fichero de tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
  - Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
  - De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición (ARCO).
  - De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

- Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mimos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

Con carácter general, cuando se recaban datos personales debe informarse a los interesados de lo expuesto anteriormente.

Derecho de acceso:

El interesado tiene derecho a solicitar y obtener gratuitamente información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

En el caso de que se reciba una solicitud de acceso de datos, es importante tener en cuenta que la Ley impone la obligación de hacer efectivo ese derecho en un plazo de un mes (este plazo se computaría desde el momento en que se haya recibido la solicitud y contando únicamente los días hábiles).

Este derecho sólo puede ser ejercitado a intervalos no inferiores a doce meses (salvo que se acredite por el interesado un interés legítimo para ejercitarlo antes de que transcurra un año desde la última vez que hizo uso del derecho).

En el momento en que se reciba un escrito solicitando ejercer el derecho de acceso, los pasos a seguir serán los siguientes:

- Comprobación de que existen datos personales del interesado en un fichero informático de la empresa.
- En caso negativo, remisión por correo al interesado de la plantilla adjunta en el anexo 18g (respuesta e inexistencia de datos).
- En caso afirmativo, remisión por correo al interesado de la plantilla adjunta en el anexo 18a, debidamente cumplimentada (respuesta derecho de acceso).

Derechos de rectificación y cancelación:

En el caso de que se reciba una solicitud de rectificación o cancelación de datos, es importante tener en cuenta que la Ley impone la obligación de hacer efectivo ese derecho en un plazo de diez días (este plazo se computaría desde el momento en que se haya recibido la solicitud y contando únicamente los días hábiles).

La rectificación o cancelación no es, a diferencia del acceso, un derecho que se pueda ejercitar sin más, sino que tiene que mediar justa causa. La Ley determina que se procederá a la cancelación o rectificación cuando el tratamiento de datos no se ajuste a lo dispuesto en ella o cuando los datos resulten incompletos o inexactos.

En el momento en que se reciba un escrito solicitando ejercer el derecho de rectificación o cancelación, los pasos a seguir serán los siguientes:

- Solicitud de rectificación:
    - Comprobación de que existen datos personales del interesado en un fichero informático de la empresa.
    - En caso negativo, remisión por correo al interesado de la plantilla adjunta en el anexo 18g (respuesta e inexistencia de datos).
    - En caso afirmativo, se procederá a la corrección de los datos y se remitirá por correo al interesado la plantilla adjunta en el anexo 18b (respuesta derecho rectificación).

- Solicitud de cancelación:

  - Comprobación de que existen datos personales del interesado en un fichero informático de la empresa.
  - En caso negativo, remisión por correo al interesado de la plantilla adjunta en el anexo 18g (respuesta e inexistencia de datos).
  - En caso afirmativo, y teniendo en cuenta la trascendencia de una solicitud de cancelación, por cuanto implica que el interesado que la realiza entiende que el tratamiento no se ajusta a lo dispuesto en la Ley, la actuación más recomendable será la de consultar con su asesor en materia de protección de datos, con el fin de valorar la solicitud formulada y sus posibles implicaciones, redactando la respuesta caso por caso sin que se pueda facilitar un estándar.

En caso de solicitud de cancelación de los datos, cuando éstos son necesarios por imperativo legal (ej: en facturación obligado por la LGT) no se suprimirán, sino que se procederá a su bloqueo hasta extinto dicho imperativo legal, para que no sean accesibles. Los datos deberán conservarse, no obstante, para el caso de que fueran solicitados por una Administración Pública, Juez o Tribunal que pudiera conocer de responsabilidades dimanantes de su tratamiento.

En los casos tanto de rectificación como de cancelación, si los datos se hubieran comunicado previamente a un tercero se le deberá notificar la rectificación o cancelación para que proceda asimismo a efectuarla.

En todos los casos (acceso, rectificación o cancelación) se archivarán las solicitudes formuladas con su fecha y copia de la contestación remitida al interesado.

Derecho de limitación (Art. 18):

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

   - El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
   - El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
   - El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
   - El interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Derecho a la portabilidad de los datos (Art. 20):

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

    - El tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

    - el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Derecho de oposición (Art. 21):

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

Anexo 18a - Respuesta cumplimentando el derecho de acceso

Muy Sr./a. nuestro/a:

Recibida su solicitud de acceso a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de lo siguiente:

Datos sobre su persona:

(indicar los datos obrantes en el fichero)

Origen de los datos:

(indicar si son datos obtenidos directamente del interesado o por comunicación de un tercero)

Comunicaciones realizadas:

(indicar, en su caso, a qué terceros se han comunicado los datos)

Sin otro particular,

En _____ , a ___ de _____ de 20___ _____

(Firma y sello de la empresa)

Anexo 18b - Respuesta a la solicitud de rectificación de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de rectificación de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de lo siguiente:

Datos sobre su persona:

(indicar los datos obrantes en el fichero)

Origen de los datos:

(indicar si son datos obtenidos directamente del interesado o por comunicación de un tercero)

Comunicaciones realizadas:

(indicar, en su caso, a qué terceros se han comunicado los datos)

Sin otro particular,

En _____, a ___ de _____ de 20___ _____

(Firma y sello de la empresa)

Anexo 18c - Respuesta a la solicitud de cancelación de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de cancelación a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos se ha procedido a su destrucción, cancelación o, en su defecto, al bloqueo por las causas legalmente establecidas.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____

(Firma y sello de la empresa)

Anexo 18d - Respuesta a la solicitud de limitación de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de limitación respecto al tratamiento de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos que hemos procedido a restringir el acceso a los mismos así como a adoptar las medidas necesarias para evitar su tratamiento y cesión.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____

(Firma y sello de la empresa)

Anexo 18e - Respuesta a la solicitud de portabilidad de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de portabilidad respecto a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de que se ha procedido a la portabilidad de todos sus datos.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____

(Firma y sello de la empresa)

Anexo 18f - Respuesta a la solicitud de oposición de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de oposición respecto a la cesión de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos que no se ha procedido a la cesión de los mismos.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____

(Firma y sello de la empresa)

Anexo 18g - Inexistencia de datos personales del interesado en los ficheros de la empresa

Muy Sr./a. nuestro/a:

Recibida su solicitud de derechos ARCO, respecto a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de que, una vez examinados los citados ficheros, hemos constatado que no existe ningún dato relativo a Ud.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____

Sara Macho Marques

Anexo 19 - Sitio web

Anexo 19a - Aviso legal

Cenval, S.L., con CIF/NIF nº: B28996551 y dirección en: C/ Ulises, 104, 28043 - Madrid (Madrid), no puede asumir ninguna responsabilidad derivada del uso incorrecto, inapropiado o ilícito de la información aparecida en las páginas web de: www.cenval.es

Que Cenval, S.L. consta inscrita en el Registro Mercantil de _____,
Tomo _____, Folio _____, Sección ___ª, Hoja _____, inscripción ___ª.

Con los límites establecidos en la ley, Cenval, S.L. no asume ninguna responsabilidad derivada de la falta de veracidad, integridad, actualización y precisión de los datos o informaciones que contienen sus páginas web.

Los contenidos e información no vinculan a Cenval, S.L. ni constituyen opiniones, consejos o asesoramiento legal de ningún tipo pues se trata meramente de un servicio ofrecido con carácter informativo y divulgativo.

Las páginas de Internet de Cenval, S.L. pueden contener enlaces (links) a otras páginas de terceras partes que Cenval, S.L. no puede controlar. Por lo tanto, Cenval, S.L. no puede asumir responsabilidades por el contenido que pueda aparecer en páginas de terceros.

Los textos, imágenes, sonidos, animaciones, software y el resto de contenidos incluidos en este website son propiedad exclusiva de Cenval, S.L. o sus licenciantes. Cualquier acto de transmisión, distribución, cesión, reproducción, almacenamiento o comunicación pública total o parcial, deberá contar con el consentimiento expreso de Cenval, S.L..

Asimismo, para acceder a algunos de los servicios que Cenval, S.L. ofrece a través del sitio web, deberá proporcionar algunos datos de carácter personal. En cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos le informamos que, mediante la cumplimentación de los presentes formularios, sus datos personales quedarán incorporados y serán tratados en los ficheros de Cenval, S.L. con el fin de poderle prestar y ofrecer nuestros servicios así como para informarle de las mejoras del sitio Web.

Le informamos también de que tendrá la posibilidad en todo momento de ejercer los derechos de acceso, rectificación, cancelación, oposición, limitación y portabilidad de sus datos de carácter personal, de manera gratuita mediante email a: cenvalsa@cenval.es o en la dirección: C/ Ulises, 104, 28043 - Madrid (Madrid).

Anexo 19b - Política de privacidad

Protección de datos de carácter personal según el RGPD

Cenval, S.L., en aplicación de la normativa vigente en materia de protección de datos de carácter personal, informa que los datos personales que se recogen a través de los formularios del Sitio web: www.cenval.es, se incluyen en los ficheros automatizados específicos de usuarios de los servicios de Cenval, S.L.

La recogida y tratamiento automatizado de los datos de carácter personal tiene como finalidad el mantenimiento de la relación comercial y el desempeño de tareas de información, formación, asesoramiento y otras actividades propias de Cenval, S.L.

Estos datos únicamente serán cedidos a aquellas entidades que sean necesarias con el único objetivo de dar cumplimiento a la finalidad anteriormente expuesta.

Cenval, S.L. adopta las medidas necesarias para garantizar la seguridad, integridad y confidencialidad de los datos conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos, y derogando la antigua LOPD, la nueva Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

El usuario podrá en cualquier momento ejercitar los derechos de acceso, oposición, rectificación, cancelación, limitación y portabilidad reconocidos en el citado Reglamento (UE). El ejercicio de estos derechos puede realizarlo el propio usuario a través de email a: cenvalsa@cenval.es o en la dirección: C/ Ulises, 104, C.P. 28043 - Madrid (Madrid).

El usuario manifiesta que todos los datos facilitados por él son ciertos y correctos, y se compromete a mantenerlos actualizados, comunicando los cambios a Cenval, S.L.

Finalidad del tratamiento de los datos personales:

¿Con qué finalidad trataremos tus datos personales?

En Cenval, S.L., trataremos tus datos personales recabados a través del Sitio Web: www.cenval.es, con las siguientes finalidades:

1. En caso de contratación de los bienes y servicios ofertados a través de www.cenval.es, para mantener la relación contractual, así como la gestión, administración, información, prestación y mejora del servicio.
2. Envío de información solicitada a través de los formularios dispuestos en www.cenval.es.
3. Remitir boletines (newsletters), así como comunicaciones comerciales de promociones y/o publicidad de www.cenval.es y del sector.

Te recordamos que puedes oponerte al envío de comunicaciones comerciales por cualquier vía y en cualquier momento, remitiendo un correo electrónico a la dirección anteriormente indicada.

Los campos de dichos registros son de cumplimentación obligatoria, siendo imposible realizar las finalidades expresadas si no se aportan esos datos.

¿Por cuánto tiempo se conservan los datos personales recabados?

Los datos personales proporcionados se conservarán mientras se mantenga la relación comercial o no solicites su supresión y durante el plazo por el cuál pudieran derivarse responsabilidades legales por los servicios prestados.

Legitimación:

El tratamiento de tus datos se realiza con las siguientes bases jurídicas que legitiman el mismo:

1. La solicitud de información y/o la contratación de los servicios de Cenval, S.L., cuyos términos y condiciones se pondrán a tu disposición en todo caso, de forma previa a una eventual contratación.
2. El consentimiento libre, específico, informado e inequívoco, en tanto que te informamos poniendo a tu disposición la presente política de privacidad, que tras la lectura de la misma, en caso de estar conforme, puedes aceptar mediante una declaración o una clara acción afirmativa, como el marcado de una casilla dispuesta al efecto.

En caso de que no nos facilites tus datos o lo hagas de forma errónea o incompleta, no podremos atender tu solicitud, resultando del todo imposible proporcionarte la información solicitada o llevar a cabo la contratación de los servicios.

Destinatarios:

Los datos no se comunicarán a ningún tercero ajeno a Cenval, S.L., salvo obligación legal.

Como encargados de tratamiento, tenemos contratados a los siguientes proveedores de servicios, habiéndose comprometido al cumplimiento de las disposiciones normativas, de aplicación en materia de protección de datos, en el momento de su contratación:

*** Nota: Para visualizar el contenido de la siguiente página será requisito previo rellenar los encargados de tratamiento. Este trámite lo podrá realizar en la pestaña "ENCARGADOS" y posteriormente haciendo click en el botón "+ Nuevo encargado".**

Datos recopilados por usuarios de los servicios

En los casos en que el usuario incluya ficheros con datos de carácter personal en los servidores de alojamiento compartido, Cenval, S.L. no se hace responsable del incumplimiento por parte del usuario del RGPD.

Retención de datos en conformidad a la LSSI

Cenval, S.L. informa de que, como prestador de servicio de alojamiento de datos y en virtud de lo establecido en la Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), retiene por un periodo máximo de 12 meses la información imprescindible para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio. La retención de estos datos no afecta al secreto de las comunicaciones y sólo podrán ser utilizados en el marco de una investigación criminal o para la salvaguardia de la seguridad pública, poniéndose a disposición de los jueces y/o tribunales o del Ministerio que así los requiera.

La comunicación de datos a las Fuerzas y Cuerpos del Estado se hará en virtud a lo dispuesto en la normativa sobre protección de datos personales.

Derechos propiedad intelectual www.cenval.es

Cenval, S.L. es titular de todos los derechos de autor, propiedad intelectual, industrial, "know how" y cuantos otros derechos guardan relación con los contenidos del sitio web www.cenval.es y los servicios ofertados en el mismo, así como de los programas necesarios para su implementación y la información relacionada.

No se permite la reproducción, publicación y/o uso no estrictamente privado de los contenidos, totales o parciales, del sitio web www.cenval.es sin el consentimiento previo y por escrito.

Propiedad intelectual del software

El usuario debe respetar los programas de terceros puestos a su disposición por Cenval, S.L., aún siendo gratuitos y/o de disposición pública.

Cenval, S.L. dispone de los derechos de explotación y propiedad intelectual necesarios del software.

El usuario no adquiere derecho alguno o licencia por el servicio contratado, sobre el software necesario para la prestación del servicio, ni tampoco sobre la información técnica de seguimiento del servicio, excepción hecha de los derechos y licencias necesarios para el cumplimiento de los servicios contratados y únicamente durante la duración de los mismos.

Para toda actuación que exceda del cumplimiento del contrato, el usuario necesitará autorización por escrito por parte de Cenval, S.L., quedando prohibido al usuario acceder, modificar, visualizar la configuración, estructura y ficheros de los servidores propiedad de Cenval, S.L., asumiendo la responsabilidad civil y penal derivada de cualquier incidencia que se pudiera producir en los servidores y sistemas de seguridad como consecuencia directa de una actuación negligente o maliciosa por su parte.

Propiedad intelectual de los contenidos alojados

Se prohíbe el uso contrario a la legislación sobre propiedad intelectual de los servicios prestados por Cenval, S.L. y, en particular de:

- La utilización que resulte contraria a las leyes españolas o que infrinja los derechos de terceros.
- La publicación o la transmisión de cualquier contenido que, a juicio de Cenval, S.L., resulte violento, obsceno, abusivo, ilegal, racial, xenófobo o difamatorio.
- Los cracks, números de serie de programas o cualquier otro contenido que vulnere derechos de la propiedad intelectual de terceros.
- La recogida y/o utilización de datos personales de otros usuarios sin su consentimiento expreso o contraviniendo lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.
- La utilización del servidor de correo del dominio y de las direcciones de correo electrónico para el envío de correo masivo no deseado.

El usuario tiene toda la responsabilidad sobre el contenido de su web, la información transmitida y almacenada, los enlaces de hipertexto, las reivindicaciones de terceros y las acciones legales en referencia a propiedad intelectual, derechos de terceros y protección de menores.

El usuario es responsable respecto a las leyes y reglamentos en vigor y las reglas que tienen que ver con el funcionamiento del servicio online, comercio electrónico, derechos de autor, mantenimiento del orden público, así como principios universales de uso de Internet.

El usuario indemnizará a Cenval, S.L. por los gastos que generara la imputación de Cenval, S.L. en alguna causa cuya responsabilidad fuera atribuible al usuario, incluidos honorarios y gastos de defensa jurídica, incluso en el caso de una decisión judicial no definitiva.

Protección de la información alojada

Cenval, S.L. realiza copias de seguridad de los contenidos alojados en sus servidores, sin embargo no se responsabiliza de la pérdida o el borrado accidental de los datos por parte de los usuarios. De igual manera, no garantiza la reposición total de los datos borrados por los usuarios, ya que los citados datos podrían haber sido suprimidos y/o modificados durante el periodo del tiempo transcurrido desde la última copia de seguridad.

Los servicios ofertados, excepto los servicios específicos de backup, no incluyen la reposición de los contenidos conservados en las copias de seguridad realizadas por Cenval, S.L., cuando esta pérdida sea imputable al usuario; en este caso, se determinará una tarifa acorde a la complejidad y volumen de la recuperación, siempre previa aceptación del usuario.

La reposición de datos borrados sólo está incluida en el precio del servicio cuando la pérdida del contenido sea debida a causas atribuibles a Cenval, S.L..

Comunicaciones comerciales

En aplicación de la LSSI. Cenval, S.L. no enviará comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

En el caso de usuarios con los que exista una relación contractual previa, Cenval, S.L. sí está autorizado al envío de comunicaciones comerciales referentes a productos o servicios de Cenval, S.L. que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el usuario, tras acreditar su identidad, podrá solicitar que no se le haga llegar más información comercial a través de los canales de Atención al Cliente.

Anexo 19c - Política de cookies

Este sitio web utiliza cookies propias y de terceros para obtener estadísticas sobre los hábitos de navegación del usuario, mejorar su experiencia y permitirle compartir contenidos en redes sociales. Usted puede aceptar o rechazar todas las cookies, así como personalizar cuáles quiere deshabilitar

Puede encontrar toda la información en nuestra Política de Cookies.

Aceptar cookies | Modificar su configuración

NOTA - Si hace clic en el botón:

"Aceptar cookies":
Continua navegando por la página web y el mensaje puede desaparecer.

"Modificar su configuración":
Accede al apartado "Cómo modificar la configuración de las cookies" del siguiente texto.

NOTA

En la siguientes páginas exponemos el texto legal para incluir en su página web advirtiendo del uso de cookies, en este caso sólo las de Google Analytics que suponemos que podrán utilizar.

En caso de que utilicen otras cookies, deben ofrecer información sobre la utilización de las cookies que se van a instalar y, en su caso, indicar los fines del tratamiento de los datos personales que se llevará a cabo a través de ellas.
Ejemplo: "cookie PHPSESSID – permite al usuario visualizar la página web e interactuar con ella".

También es necesario que incluyan un aviso como el del ejemplo al entrar en la página web, antes de que se le instalen las cookies al usuario.

TEXTO LEGAL PARA INCLUIR EN LA WEB (CAPA 2)

Política de cookies

Cenval, S.L. informa acerca del uso de las cookies en su página web: www.cenval.es

¿Qué son las cookies?

Las cookies son archivos que se pueden descargar en su equipo a través de las páginas web. Son herramientas que tienen un papel esencial para la prestación de numerosos servicios de la sociedad de la información. Entre otros, permiten a una página web almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo y, dependiendo de la información obtenida, se pueden utilizar para reconocer al usuario y mejorar el servicio ofrecido.

Tipos de cookies

Según quien sea la entidad que gestione el dominio desde donde se envían las cookies y trate los datos que se obtengan se pueden distinguir dos tipos:

- Cookies propias:
  Aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario.

- Cookies de terceros:
  Aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las cookies.

En el caso de que las cookies sean instaladas desde un equipo o dominio gestionado por el propio editor pero la información que se recoja mediante éstas sea gestionada por un tercero, no pueden ser consideradas como cookies propias.

Existe también una segunda clasificación según el plazo de tiempo que permanecen almacenadas en el navegador del cliente, pudiendo tratarse de:

- Cookies de sesión:
  Diseñadas para recabar y almacenar datos mientras el usuario accede a una página web. Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (p.e. una lista de productos adquiridos).

- Cookies persistentes:
  Los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años.

Por último, existe otra clasificación con seis tipos de cookies según la finalidad para la que se traten los datos obtenidos:

- Cookies técnicas:
  Aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan como, por ejemplo, controlar el tráfico y la comunicación de datos, identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, realizar la solicitud de inscripción o participación en un evento, utilizar elementos de seguridad durante la navegación, almacenar contenidos para la difusión de vídeos o sonido o compartir contenidos a través de redes sociales.

- Cookies de personalización:
  Permiten al usuario acceder al servicio con algunas características de carácter general predefinidas en función de una serie de criterios en el terminal del usuario como por ejemplo serian el idioma, el tipo de navegador a través del cual accede al servicio, la configuración regional desde donde accede al servicio, etc.

- Cookies de análisis:
  Permiten al responsable de las mismas, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida mediante este tipo de cookies se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.

- Cookies publicitarias:
  Permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios.

- Cookies de publicidad comportamental:
  Almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.

- Cookies de redes sociales externas:
  Se utilizan para que los visitantes puedan interactuar con el contenido de diferentes plataformas sociales (facebook, youtube, twitter, linkedIn, etc..) y que se generen únicamente para los usuarios de dichas redes sociales. Las condiciones de utilización de estas cookies y la información recopilada se regula por la política de privacidad de la plataforma social correspondiente.

Desactivación y eliminación de cookies

Tienes la opción de permitir, bloquear o eliminar las cookies instaladas en tu equipo mediante la configuración de las opciones del navegador instalado en su equipo. Al desactivar cookies, algunos de los servicios disponibles podrían dejar de estar operativos. La forma de deshabilitar las cookies es diferente para cada navegador, pero normalmente puede hacerse desde el menú Herramientas u Opciones. También puede consultarse el menú de Ayuda del navegador dónde puedes encontrar instrucciones. El usuario podrá en cualquier momento elegir qué cookies quiere que funcionen en este sitio web.

Puede usted permitir, bloquear o eliminar las cookies instaladas en su equipo mediante la configuración de las opciones del navegador instalado en su ordenador:

- Microsoft Internet Explorer o Microsoft Edge:
  http://windows.microsoft.com/es-es/windows-vista/Block-or-allow-cookies

- Mozilla Firefox:
  http://support.mozilla.org/es/kb/impedir-que-los-sitios-web-guarden-sus-preferencia

- Chrome:
  https://support.google.com/accounts/answer/61416?hl=es

- Safari:
  http://safari.helpmax.net/es/privacidad-y-seguridad/como-gestionar-las-cookies/

- Opera:
  http://help.opera.com/Linux/10.60/es-ES/cookies.html

Además, también puede gestionar el almacén de cookies en su navegador a través de herramientas como las siguientes

- Ghostery:
  www.ghostery.com/

- Your Online Choices:
  www.youronlinechoices.com/es/

Cookies utilizadas en www.cenval.es

A continuación se identifican las cookies que están siendo utilizadas en este portal así como su tipología y función:

Aceptación de la Política de cookies

www.cenval.es, asume que usted acepta el uso de cookies. No obstante, muestra información sobre su Política de cookies en la parte inferior o superior de cualquier página del portal con cada inicio de sesión con el objeto de que usted sea consciente.

Ante esta información es posible llevar a cabo las siguientes acciones:

- Aceptar cookies:
  No se volverá a visualizar este aviso al acceder a cualquier página del portal durante la presente sesión.

- Cerrar:
  Se oculta el aviso en la presente página.

- Modificar su configuración:
  Podrá obtener más información sobre qué son las cookies, conocer la Política de cookies de: www.cenval.es y modificar la configuración de su navegador.

Anexo 20 - Comunicaciones

Anexo 20a - Correo electrónico

Este mensaje va dirigido, de manera exclusiva, a su destinatario y puede contener información confidencial y sujeta al secreto profesional, cuya divulgación no está permitida por Ley.

En caso de haber recibido este mensaje por error, le rogamos que de forma inmediata, nos lo comunique mediante correo electrónico remitido a nuestra atención y proceda a su eliminación, así como a la de cualquier documento adjunto al mismo.

Asimismo, le comunicamos que la distribución, copia o utilización de este mensaje, o de cualquier documento adjunto al mismo, cualquiera que fuera su finalidad, están prohibidas por la ley.

En aras del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, puede ejercer los derechos de acceso, rectificación, cancelación, limitación, oposición y portabilidad de manera gratuita mediante correo electrónico a: cenvalsa@cenval.es o bien en la siguiente dirección: C/ Ulises, 104, C.P. 28043, Madrid (Madrid).

Anexo 20b - Fax

La información transmitida en este telefax va dirigida únicamente a la persona o entidad que se muestra como destinatario y puede contener datos confidenciales o privilegiados.

Toda revisión, retransmisión, diseminación u otro uso o acción al respecto por parte de personas o entidades distintas al destinatario está prohibida por Ley.

En caso de haber recibido este telefax por error, le rogamos que de forma inmediata, nos lo comunique al número de teléfono 917216010 y proceda a su eliminación.

En aras del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, puede ejercer los derechos de acceso, rectificación, cancelación, limitación, oposición y portabilidad de manera gratuita mediante correo electrónico a: cenvalsa@cenval.es o bien en la siguiente dirección: C/ Ulises, 104, C.P. 28043, Madrid (Madrid).

Anexo 20c - Facturas

Sus datos de carácter personal han sido recogidos de acuerdo con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.

Le ponemos en conocimiento que estos datos se encuentran almacenados en un fichero propiedad de Cenval, S.L..

De acuerdo con la Ley anterior, tiene derecho a ejercer los derechos de acceso, rectificación, cancelación, limitación, oposición y portabilidad de manera gratuita mediante correo electrónico a: cenvalsa@cenval.es o bien en la siguiente dirección: C/ Ulises, 104, C.P. 28043, Madrid (Madrid).

.....

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

Si utilizara sus datos con fines distintos a los necesarios para el servicio contratado (enviar publicidad, suscripción a un boletín informativo...) y/o recoge datos especialmente protegidos (de salud, sexualidad, afiliación política, religiosos...) será necesario notificárselo a sus clientes y que FIRMEN la CLAUSULA DE CONSENTIMIENTO EXPRESO.

DOCUMENTO DE SEGURIDAD

PARA EL TRATAMIENTO DE DATOS DE CARACTER PERSONAL

CENVAL, S.L.