

ANEXO AL CONTRATO LABORAL

CLÁUSULAS ADICIONALES: OBLIGACIONES DEL EMPLEADO

1. CONFIDENCIALIDAD

1.1. A los efectos de esta cláusula, información confidencial incluirá toda información y documentación relativa al negocio y/o a las materias financieras de la Empresa y de los agentes, clientes, clientes potenciales o proveedores de la misma y, en concreto, comprenderá:

1.1.1. Los métodos comerciales e información de la Empresa (incluidos precios, descuentos concedidos a los clientes u obtenidos de proveedores, desarrollos de productos, programas de marketing y publicidad, cálculos de costes, presupuestos, objetivos de ventas o cualquier otra información financiera);

1.1.2. Listas y datos de proveedores, clientes y clientes potenciales de la Empresa;

1.1.3. Datos y condiciones de los contratos con proveedores y clientes de la Empresa;

1.1.4. Procesos secretos de fabricación o producción y know how utilizados por la Empresa o sus proveedores;

1.1.5. Datos confidenciales relativos a cualquier activo intangible de la Empresa, incluidos, entre otros, marcas, derechos de propiedad intelectual, diseños de productos, patentes o desarrollos de futuros productos de la Empresa, así como de los proveedores de la misma;

1.1.6. Datos de cualesquiera promociones o futuras promociones, o ejercicios de marketing o de publicidad planeados por la Empresa;

1.1.7. Datos de cualesquiera presupuestos o planes de negocio de la Empresa;

1.1.8. Toda información que pueda afectar al valor del negocio o de las acciones de la Empresa, con independencia de que en el caso de documentos o de otros materiales escritos o de cualesquiera materiales en formato electrónico, sean o no, o se encuentren señalados o no, como confidenciales, y con independencia de que, en el caso de otra información, la Empresa trate dicha información o no como confidencial; y

1.1.9. Cualesquiera otros datos, documentación e información no recogidos en los apartados anteriores relativos a la Empresa que sean considerados como secreto comercial, sean confidenciales o comercialmente sensibles y/o que no se encuentre fácilmente a disposición de terceros en negocios similares al de la Empresa o del público en general, y que, en caso de ser revelada, pueda causar un daño a la Empresa.

En adelante, todo ello denominado **“INFORMACIÓN CONFIDENCIAL”**.

1.2. El Empleado reconoce que en el transcurso ordinario de su relación laboral con la Empresa podrá tener acceso a Información Confidencial. Por lo tanto, el Empleado mediante la firma del presente Anexo acepta mantenerla en secreto y asume los compromisos y las restricciones establecidas en los párrafos que siguen a continuación.

1.3. Mientras su contrato laboral con la Empresa esté en vigor, el Empleado se compromete a no obtener ni tratar de obtener ninguna ventaja económica ni competitiva de ningún tipo (directa o indirecta) con la revelación, descarga, carga, copia, transmisión, retirada o destrucción de información, especialmente de Información Confidencial, adquirida por él mismo en el transcurso de su relación laboral.

1.4. En ningún momento durante la vigencia del contrato laboral con la Empresa, ni con posterioridad a su extinción, el Empleado utilizará ni revelará directa o indirectamente, excepto previa aprobación por escrito de una persona apoderada de la Empresa y siempre en beneficio de ésta última, secretos comerciales ni información confidencial propiedad de o relativa a la Empresa, o a los agentes, clientes, clientes potenciales o proveedores de la Empresa.

1.5. No se impedirá que el Empleado utilice o revele cualquier Información Confidencial que:

1.5.1. Esté autorizado a utilizar o revelar por su superior inmediato; o

1.5.2. Haya pasado a ser de dominio público salvo que haya sido como resultado de una revelación no autorizada por parte del Empleado o de un tercero empleado o contratado por la Empresa; o

1.5.3. Deba revelar por ley.

1.6. El Empleado no realizará copias de ningún documento, memorando, correspondencia, disco de ordenador, CD-ROM, tarjeta de memoria, cinta de video o cualquier materia similar (incluido, a efectos aclaratorios, en cualquier formato electrónico) ni sacará ninguno de dichos artículos de las instalaciones de la Empresa de forma distinta a en el adecuado cumplimiento de sus funciones en virtud del contrato, excepto con la autorización escrita del superior inmediato del Empleado, cuya autorización será válida exclusivamente en dicha instancia.

1.7. El Empleado no efectuará ninguna manifestación pública negativa (ya sea escrita o verbal) a los medios, vía redes sociales, ni de ninguna otra forma, en relación con los asuntos de la Empresa, y no escribirá ningún artículo para ser publicado sobre ninguna materia relacionada con el negocio de la misma, ni con otros asuntos de la Empresa sin la previa autorización escrita del CEO de la Empresa.

2. PROPIEDAD INTELECTUAL E INDUSTRIAL

2.1. El Empleado es consciente y acepta que, conforme a los artículos 51 y 97.4 de la Ley de Propiedad Intelectual, los derechos sobre cualesquiera creaciones que hubiese desarrollado en el contexto de la relación laboral pertenecerán automática y exclusivamente a la Empresa.

2.2. Además de lo anterior, el Empleado acepta cooperar con la Empresa de una forma segura y eficiente para garantizar que todos los derechos sobre las creaciones que hubiese desarrollado sean debidamente conferidos a la Empresa, puedan ser protegidos y disfrutados por la misma.

2.3. Por lo tanto, el Empleado acepta el derecho exclusivo de la Empresa a inscribir a su propio nombre y en su favor cualesquiera creaciones que hubiese desarrollado en el contexto de la relación laboral.

2.4. Se entenderá que el salario recibido por el Empleado incluye toda compensación de cualquier tipo a la que pueda tener derecho en relación con el desarrollo de activos de propiedad intelectual e industrial.

3. USO DE LOS SISTEMAS INFORMÁTICOS

3.1. La Empresa proporcionará al Empleado los sistemas informáticos (acceso a Internet, correo electrónico, etc.) que puedan ser necesarios para cumplir con las funciones correspondientes a su puesto de trabajo conforme a las necesidades y actividad de la Empresa. Por ello:

3.1.1. La utilización de estas herramientas será exclusivamente a efectos del desarrollo de sus funciones dada su condición de herramientas profesionales;

3.1.2. No obstante lo anterior, se aceptará el uso personal de estas herramientas en la medida en que se limite a lo mínimo y estrictamente necesario y, en ningún caso podrá el Empleado mirar, descargar, enviar ni recibir ningún tipo de material indecoroso o inadecuado para su desempeño profesional, ni ningún otro tipo de material ilícito.

3.2. Si la Empresa detectara que el Empleado utiliza inadecuadamente dichas herramientas profesionales, mira,

descarga, envía o recibe material indecoroso o inadecuado u otro tipo de material ilícito, o si la Empresa descubriera que el Empleado ha incumplido las medidas de seguridad en vigor de los sistemas de información de la Empresa, ésta podrá adoptar las medidas disciplinarias adecuadas, incluido el despido disciplinario. Asimismo, la Empresa podrá iniciar las correspondientes acciones como consecuencia de los daños generados, directa o indirectamente, por cualquier incumplimiento en esta materia.

3.3. Lo anteriormente expuesto no se verá afectado por el hecho de que el Empleado obtenga o no un beneficio personal o que la Empresa incurra o no en pérdidas.

3.4. Con el fin de examinar la aplicación de lo anterior y de ejercer un control laboral, para garantizar la seguridad de la información y de los sistemas de información de la Empresa y para mantener la comunicación cuando el Empleado se encuentre ausente (por ejemplo, debido a enfermedad o vacaciones) o cuando no pueda garantizarse la comunicación de otra forma (por ejemplo, a través de funciones de respuesta automática o de redirección), la Empresa podrá acceder a las comunicaciones electrónicas del Empleado (correo electrónico e Internet) y controlar su utilización por el Empleado.

3.5. Por todo lo anterior, el Empleado acepta y autoriza expresamente a la Empresa a acceder a la cuenta de correo electrónico que le haya asignado la Empresa o al historial de páginas web visitadas por el Empleado, en la medida en que este acceso sea puntual y estrictamente necesario para cumplir con las necesidades anteriormente citadas.

4. PROPIEDAD DE LA COMPAÑÍA

4.1. El Empleado hará todo lo posible para cuidar todos los documentos, artículos y materiales que pueda recibir de la Empresa, y para conservarlos en buenas condiciones.

4.2. En el supuesto de que el contrato se extinga por cualquier causa, el Empleado se compromete a devolver a la Empresa toda la Información Confidencial, documentación y archivos de cualquier tipo relativos a la actividad y al negocio de la Empresa o a sus clientes, o a destruirla si así se lo solicitasen.

4.3. Asimismo, en el supuesto de extinción del contrato por cualquier motivo, el Empleado entregará a la Empresa todos los objetos que haya recibido de la misma, incluidos, entre otros [vehículo de empresa, móvil, hardware y software, tarjetas de crédito, llaves del centro de trabajo, etc.,] así como cualquier otra propiedad de la Empresa que pueda estar en posesión o control del Empleado.

5. INFORMACIÓN AL EMPLEADO SOBRE EL TRATAMIENTO DE SUS DATOS

5.1. ¿Quién es el responsable del tratamiento de sus datos?

Identidad: COMPAÑÍA EUROPEA DE VIAJEROS ESPAÑA, S.A., sociedad española, con CIF número A81544868

Dirección postal: Avda. Petróleo 28 - 28918 Leganés (Madrid)

Teléfono: 915393132

E-mail: info@cevesa.es

5.2. ¿Con qué finalidad tratamos sus datos personales?

La Empresa trata la información facilitada por Ud. con el fin de llevar a cabo:

- a) La gestión de sus nóminas.
- b) Llevar a cabo la correcta gestión contable de la entidad.
- c) Evaluación del desempeño.
- d) Planificación y gestión de cursos de formación.
- e) Cumplir con las obligaciones derivadas de la normativa referente a la prevención de riesgos laborales y transporte por carretera (en el caso de los conductores).
- f) Cumplir con las obligaciones derivadas de la normativa referente a la seguridad social (en materia de afiliación, altas, bajas o variaciones que, en su caso, se produzcan).
- g) Control del cumplimiento de las obligaciones y deberes laborales. La supervisión de la actividad del trabajador podrá llevarse a cabo, en caso de ser necesario, a través de la revisión de las

comunicaciones realizadas por cualquier medio (email, fax, correo, etc.) o el uso de sistemas de control.

h) Control del cumplimiento del horario laboral y de acceso a las instalaciones a través de un sistema de fichaje por tarjeta magnética y/o huella dactilar.

i) Mantenimiento de la seguridad, control interno de las instalaciones y supervisión laboral de los trabajadores a través de un sistema de videovigilancia.

5.3. ¿Por cuánto tiempo conservaremos sus datos?

Los datos facilitados serán tratados por la Empresa mientras persista la relación laboral. Transcurrido este plazo, los datos necesarios pasarán a permanecer bloqueados para el cumplimiento de las obligaciones establecidas a efectos laborales durante un plazo de CUATRO (4) AÑOS, a efectos fiscales durante un plazo de DIEZ (10) AÑOS y a efectos contables durante un plazo de SEIS (6) AÑOS.

Los fichajes a través de huella dactilar se conservarán mientras exista un interés legítimo de la Empresa para la realización de controles laborales, y en todo caso durante un periodo máximo de 3 años una vez finalizada la relación laboral.

Las imágenes captadas por las cámaras de videovigilancia se conservarán un máximo de 30 días naturales.

5.4. ¿Cuál es la legitimación para el tratamiento de sus datos?

La ejecución de un contrato laboral: el tratamiento es necesario para la ejecución del contrato laboral suscrito entre el Empleado y el responsable del tratamiento, es decir, la Empresa.

El cumplimiento de obligaciones legales: el tratamiento es necesario para el cumplimiento de las obligaciones laborales, fiscales y contables establecidas en el art. 21 del RDL 5/2000, art. 66 Bis de la LGT y art. 30 del Código Comercio.

El tratamiento de los datos registrados por los tacógrafos tiene su base legal en el Reglamento UE 165/2014.

El interés legítimo del Responsable: el tratamiento de la huella dactilar y todos los sistemas de control laboral están legitimados por el interés legítimo del Responsable y por lo establecido en el artículo 20.3 del Estatuto de Trabajadores "El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso."

El tratamiento de las imágenes grabadas por las cámaras de videovigilancia está legitimado por el interés legítimo del responsable, según lo previsto en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras y el art. 20.3 del Estatuto de los Trabajadores para la seguridad y control de acceso a las instalaciones y para llevar un control de la actividad interna desarrollada en la Empresa.

5.5. ¿A qué destinatarios se comunicarán sus datos?

Los datos facilitados por el Empleado podrán ser cedidos a los organismos de la Seguridad Social correspondientes; a la Administración Tributaria; bancos, cajas de ahorro y cajas rurales, entidades aseguradoras correspondientes, Fuerzas y Cuerpos de Seguridad, Órganos Judiciales o a otras administraciones públicas que puedan resultar competentes en la materia.

5.6. ¿Cuáles son sus derechos cuando nos facilita los datos?

Cualquier persona tiene derecho a obtener información sobre si la Empresa está tratando datos personales que le conciernen o no y, en tal caso, a ejercer su derecho de acceso a los datos personales y a la siguiente información:

- a) los fines del tratamiento;
- b) las categorías de datos personales de que se trate;
- c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular, destinatarios en terceros u organizaciones internacionales;
- d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- e) la existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de datos

personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control. Asimismo, el Empleado tiene derecho a solicitar la rectificación de los datos inexactos o, en su caso, a solicitar la supresión de los mismos cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos o cuando decida retirar el consentimiento en que se hubiera basado el tratamiento hasta la fecha. El Empleado podrá además solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente serán conservados por la Compañía para el ejercicio o la defensa de reclamaciones. La Empresa dejará de tratar sus datos siempre que el Empleado lleve a cabo la oposición a dicho tratamiento, salvo por motivos legítimos imperiosos, o por el ejercicio o la defensa de posibles reclamaciones. Finalmente, y en ejercicio de su derecho a la portabilidad de los datos, el Empleado podrá recibir los datos personales que hubiera proporcionado a la Empresa, en un formato estructurado, de uso común y legible por máquina, así como a solicitar que se transmitan a otra entidad responsable del tratamiento.

5.7. ¿Cómo puede el Empleado ejercer materialmente estos derechos?

Usted podrá ejercer materialmente los derechos descritos en el apartado anterior solicitando el correspondiente formulario a la dirección del responsable: info@cevesa.es. Adicionalmente, le informamos que usted podrá solicitar información en todo momento acerca del ejercicio de los derechos que le incumben ante la Agencia Española de Protección de Datos. En caso de que el ejercicio de sus derechos no hubiera sido atendido o satisfecho correctamente, le informamos de que usted podrá presentar la correspondiente reclamación ante la Agencia Española de Protección de Datos, ubicada en la Calle de Jorge Juan, 6, 28001, Madrid, teléfono 912663517. Y para que conste a los efectos oportunos, en prueba de conformidad de las partes, firman el presente acuerdo, por duplicado, en el lugar y la fecha indicados en el encabezamiento.

6. POLÍTICA DE SEGURIDAD: FUNCIONES Y OBLIGACIONES DEL EMPLEADO

El Empleado deberá actuar en todo momento conforme las instrucciones detalladas en el presente documento. Para ello se establecen las siguientes medidas de protección de datos que el Empleado se obliga a cumplir expresamente:

6.1. Organización de la información

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

6.2. Conservación de los datos

Se deberán conservar los datos en el mobiliario y departamento destinados a tal fin. Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por el Responsable de Seguridad. No está permitido conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo ser conservados en el lugar apropiado al término de la jornada laboral.

6.3. Acceso a la información

Se deberán aplicar los mecanismos de acceso restringido a la información que haya implementado la organización, salvaguardando las claves de acceso de toda divulgación o comunicación a otras personas. El Empleado sólo está autorizado a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones. Se restringirá el acceso a los equipos informáticos mediante procedimientos de puedan identificar y autenticar la persona que accede a los mismos. Los nombres de usuario y contraseña tendrán la consideración de datos personales intransferibles.

6.4. Procesamiento de datos

Los soportes documentales e informáticos deberán estar dispuestos de tal forma que no sean accesibles a personas no autorizadas. Si una persona abandona su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador, de modo que se impida la visualización de la información con la que estaba trabajando. Cuando se utilicen impresoras o fotocopadoras, después de la impresión de trabajos con información de carácter personal, se debe recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

6.5. Transporte de soportes

El transporte de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado o empresas externas contratadas para tal fin por la Compañía.

6.6. Eliminación de documentos

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

6.7. Copia de seguridad y recuperación de datos

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

6.8. Protección de datos

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

6.9. Gestión de incidencias

Se considera una incidencia a cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales. El Empleado tiene la obligación de notificar sin demora injustificada, cualquier incidencia que tenga conocimiento al Responsable de Seguridad de la Empresa para su conocimiento y aplicación de medidas correctivas para remediar y mitigar los efectos que hubiera podido ocasionar. Las incidencias deberán documentarse por la persona que la notifica con una descripción detallada de la misma y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella. El conocimiento y no notificación de una incidencia por parte del Empleado se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que el Responsable se vea obligado a atender como consecuencia de dicho incumplimiento.

6.10. Salvaguarda y protección de las contraseñas personales

Están expresamente prohibidas las siguientes actividades:

- a) Compartir o facilitar el identificador de usuario y la clave de acceso (contraseña) facilitado por la Empresa a otra persona física o jurídica. Si el Empleado sospecha que otra persona conoce sus datos de identificación y acceso deberá notificar al Responsable de Seguridad de esta incidencia para activar los mecanismos de cambio de contraseña. En caso de incumplimiento de esta prohibición, el Empleado será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada su identificación.
- b) Intentar distorsionar o falsear los registros log del sistema.
- c) Intentar aumentar o disminuir el nivel de privilegios del Empleado en el sistema.

6.11. Acceso a redes

Están expresamente prohibidas las siguientes actividades:

- a) Utilizar los datos, la red corporativa y/o la intranet de la Empresa y/o de terceros para incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la organización y/o de terceros o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.
- b) Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Empresa.
- c) Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Empresa y/o de terceros.
- d) Almacenar datos de carácter personal en el disco duro del ordenador, debiendo ser utilizadas para tal fin las carpetas de la red corporativa asignadas por la Empresa.
- e) Obstaculizar voluntariamente el acceso de otros empleados a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la organización, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.