

## **Carta informativa para el tratamiento de datos de carácter personal**

Desde IRCO, SL nos preocupamos mucho por garantizar el derecho a la protección de datos de carácter personal, por ello, en el presente documento explicamos el tratamiento que realizados de tus datos como trabajador

**Definición de dato personal:** Primero, como "Dato Personal" debemos entender cualquier información concerniente a una persona física identificada o identificable. Entre otros, se Incluyen el nombre, apellidos, la dirección postal y electrónica, así como el número de teléfono.

**Qué empresa es la responsable de los tratamientos de los datos personales:** Los datos personales recogidos durante el proceso de selección, durante el proceso de contratación y durante la vigencia de la relación laboral, serán tratados por IRCO, SL, (en adelante IRCO) en calidad de responsable del tratamiento.

**Tratamientos y finalidades de los datos recogidos:** A continuación detallamos las finalidades con las que utilizamos tus datos personales

**1.- Para el desarrollo de la relación laboral:** Lo que implica tratar los datos para el cumplimiento de las obligaciones fiscales y laborales que de ella se desprenden; confección de nóminas y tareas administrativas derivadas de la propia relación laboral; Control de la Jornada laboral; Gestión de la prevención de riesgos Realización de acciones formativas.

**Legitimación para el tratamiento de sus datos:** La base jurídica para el tratamiento de tus datos reside en el propio consentimiento manifestado para la relación laboral en base a las finalidades expuestas, así como la necesidad del tratamiento de los mismos para la ejecución de las obligaciones legales en materia laboral y fiscal.

**Plazo de conservación de los datos:** Los datos necesarios para el desarrollo de la relación laboral se mantendrán durante el tiempo necesario en base al cumplimiento con las obligaciones fiscales y laborales.

**Comunicación de sus datos personales a terceros:** Los datos personales necesarios para llevar a cabo la relación laboral sólo serán cedidos a las organizaciones públicas como la seguridad social y Agencia Tributaria que resulten necesarias por imperativo legal.

**2.- Videovigilancia:** En algunas instalaciones o centros de trabajo de la empresa se encuentran instalados diferentes sistemas de seguridad dotados de cámaras de seguridad con la finalidad de controlar las dependencias y bienes de la empresa para evitar y/o identificar la comisión de actos delictivos. Así como para realizar cuantas acciones disciplinarias sean oportunas en el caso de detectar comisiones delictivas por parte de los empleados

**Legitimación para el tratamiento de sus datos:** La base jurídica para el tratamiento de tus datos reside en el interés de la empresa para velar por la integridad de sus bienes acorde al art. 6.1.e) del Reglamento Europeo de Protección..

**Plazo de conservación de los datos:** Los datos de las imágenes se conservarán hasta el tiempo máximo permitido.

**Comunicación de sus datos personales a terceros:** Los datos captados por los sistemas de seguridad podrán ser comunicados a las fuerzas y cuerpos de seguridad del estado.

**Derechos de los usuarios:** Cuando proceda, podrás ejercitar los derechos otorgados por la normativa de protección de datos, como el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, y oposición mediante escrito, acompañado de documento identificativo, dirigido a IRCO, SL, en el domicilio de la empresa. Y en el caso de que lo estimes oportuno, podrás presentar una reclamación ante la Agencia Española de Protección de Datos.

**Seguridad en el tratamiento de datos personales:** En IRCO tenemos una preocupación especial por garantizar la seguridad de cualquier tipo de información, sean datos personales o no. Por ello la

empresa ha implantado medidas de seguridad, técnicas y organizativas, para prevenir cualquier pérdida o uso no autorizado por terceros.

Así mismo, la ejecución de las funciones encomendadas siempre se realizará cumpliendo con la debida diligencia y confidencialidad. En este aspecto, sobre los medios tecnológicos que IRCO ponga, o pudiera poner, a su disposición con el fin de que pueda llevar a cabo las funciones que le son encomendadas en virtud de su puesto de trabajo (ordenador, correo electrónico, conexión a Internet, etc.), éstos no podrán utilizarse para otros fines distintos a los que se circunscriben dentro de la propia relación laboral, quedando de este modo limitada la posibilidad de utilizar dichos medios para usos personales. Reservándose IRCO el derecho a acceder al contenido de los mismos para verificar su estado y evitar daños en los sistemas de información.

En vista de estas manifestaciones le exponemos el compromiso de confidencialidad que deberá respetar y la política de recursos informáticos establecida en IRCO:

**I.- Compromiso de confidencialidad:** Se compromete a guardar secreto sobre los datos de carácter personal y cualesquiera otras informaciones o circunstancias relativas a personas cuyos datos conozca y/o pueda tener acceso en el ejercicio de las funciones que le hubiesen sido asignadas o que, aun sin asignación formal, haya tenido que asumir en IRCO.

A estos efectos, se considerará confidencial:

- a) Toda información obtenida o remitida a través de cualquier medio de comunicación como, por ejemplo, correo postal o electrónico, teléfono, fax, así como accesos remotos y cualesquiera otras comunicaciones relacionadas con la actividad de IRCO, el resto de los trabajadores, sus clientes y colaboradores.
- b) El contenido de todas las actividades que usted desarrolle como parte de sus funciones para IRCO, con independencia de que los medios de producción utilizados hayan sido puestos a su disposición por aquélla o sean propios del firmante. En especial, tendrán la condición de confidencial los datos personales de los clientes y cualesquiera informaciones que permitan conocer su identidad o acceder a perfiles de usuario en cuentas de cualquier naturaleza
- c) En general, toda la información recogida documentos, correspondencia o cualesquiera otros soportes, automatizados o no, a los que el firmante tenga acceso con motivo de su relación con IRCO.

De manera especial, y en relación a dicha información confidencial, el firmante se obliga a:

- No transportar documentación, con independencia de que sea o no confidencial, original o copia, salvo autorización expresa de IRCO, o que así lo requiera la naturaleza de la relación con el cliente y/o el lugar donde éste se encuentre. En tales casos, deberán adoptarse las medidas de seguridad necesarias a fin de evitar pérdidas de información y accesos no autorizados.
- No transmitir, exhibir, comentar, copiar, reproducir, glosar o, bajo cualquier forma, comunicar esa información a personas ajenas a IRCO
- No utilizar para actividades distintas a su relación laboral la información a la que haya tenido acceso con motivo de la misma.

Estas obligaciones existirán también respecto a cualquier otra información, documentación y/o dato, aunque no sea de carácter personal, a los que tenga acceso con ocasión de la indicada relación laboral.

En caso de tener acceso a algún fichero que contenga datos de carácter personal con ocasión del trabajo que va a desarrollar, se obliga a recibir y leer toda la documentación relativa a la seguridad en

la información que le sea facilitada y en la que se desarrollan todos los derechos y obligaciones respecto a dicho acceso y tratamiento de datos.

**II.- Política recursos tecnológicos:** Respecto a los medios tecnológicos y de producción que IRCO ponga a su disposición para que pueda llevar a cabo sus funciones, éstos no podrán utilizarse para fines ajenos a la relación laboral, por lo que no podrán destinarse a usos personales. En particular, tanto el ordenador como el correo electrónico que se le pudiera asignar es de carácter corporativo y su uso se limita al desarrollo de las funciones profesionales que se le encarguen, reservándose IRCO el derecho a acceder a su contenido para verificar su estado y evitar daños en los sistemas de información.

En caso de que usted utilice, como herramienta de trabajo, ordenador, teléfono móvil, tablet o cualquier otro dispositivo personal, se requerirá el cumplimiento estricto de las siguientes pautas:

1.- Mantener en secreto sus claves de acceso al sistema, debiendo poner en conocimiento del departamento de informática cuando el mismo haya sido vulnerado.

2.- Solo se podrá acceder a los contenidos Web directamente relacionados con el trabajo. El acceso a Internet es una herramienta facilitada por IRCO, solo para aquellos usuarios que se les permita. IRCO establecerá mecanismos de control que permitirá controlar a que páginas webs ha accedido cada usuario / pc. Dichos mecanismos de control se notificarán y explicarán a todos los empleados.

3.- Queda prohibido la instalación de programas en la red corporativa y/o ordenador personal que no guarden relación con la actividad y objetivos de IRCO.

4.- El usuario se compromete a respetar en todo momento la legislación vigente en materia de propiedad intelectual y a hacer uso adecuado del servicio de acceso a Internet, manteniendo un comportamiento respetuoso con el resto de usuarios. Queda prohibido la instalación y manejo de programas p2p.

5.- Las contraseñas de acceso al sistema son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida.

El sistema de información cuenta con un registro de accesos activado en determinado tipo de ficheros. Salvo prueba en contrario, se presumirá que los actos realizados por el identificador asignado al usuario han sido realizados por su titular, debiendo éste responder de las irregularidades o infracciones cometidas.

6.- Cambiar la contraseña con la periodicidad requerida por el sistema.

7.- Cerrar o bloquear la sesión al término de la jornada laboral.

8.- Bloquear la sesión del usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas a su ordenador.

9.- Comunicar al departamento de informática las incidencias de seguridad de las que tenga conocimiento.

10.- No copiar la información contenida en los ficheros en los que se almacenan datos de carácter personal a disquetes o a cualquier otro soporte sin autorización expresa del Responsable de seguridad, ni extraerla de las oficinas.

11.- Guardar todos los ficheros de carácter personal empleados por el usuario en la carpeta indicada por los administradores del sistema, a fin de facilitar la realización de las copias de seguridad y proteger su acceso de personas no autorizadas.

12.- Guardar todos los soportes físicos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

13.- Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora, ni en sitios accesibles por personal ajeno a IRCO (mostrador, mesas donde se realicen reuniones y visitas).

14.- Utilizar la destructora de papel, para destruir listados y resto de documentación no precisa u obsoleta.

15.- No reutilizar el papel que contenga datos de carácter personal.

16.- Únicamente las personas autorizadas para ello en el listado de accesos autorizados podrán introducir, modificar o anular los datos contenidos en los programas de gestión. Los permisos de acceso de los usuarios son concedidos por el departamento informático. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a secciones cuyo acceso no está autorizado, deberá ponerlo en conocimiento del departamento de informática.

17.- El correo electrónico es corporativo, del tipo nombre@empresa.com. Este correo es una herramienta de trabajo propiedad de IRCO, que facilita a cada uno de los trabajadores. Este correo se utilizará única y exclusivamente para la relación con clientes, proveedores, compañeros y demás contactos en el ámbito estrictamente profesional y laboral.

Se recomienda el uso del correo electrónico para las notificaciones entre compañeros, a efectos de demostración de que se ha efectuado dicha notificación.

18.- Queda prohibido:

- Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.
- Intentar modificar o acceder al registro de accesos.
- Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.
- Utilizar Internet para tareas que no estén relacionadas directamente con las funciones asignadas al usuario.
- Introducir programas en la red corporativa y/o ordenador personal que no guarden relación con la actividad y objetivos de la compañía.
- Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de IRCO, o bien para la realización de actos que pudieran ser considerados ilícitos

**Incumplimiento:** El incumplimiento de estos compromisos podrá ser considerado falta muy grave en el ámbito laboral.

Por la presente, D. \_\_\_\_\_ he leído y soy consciente de las manifestaciones arriba expresadas.

Firma:

DNI:

Fecha: