**COMPROMISO DE CONFIDENCIALIDAD DEL TRABAJADOR**

Funciones y obligaciones de trabajadores con acceso a datos de carácter personal de la empresa \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ÁMBITO DE APLICACIÓN**

Las medidas de seguridad previstas en el presente documento son de aplicación al personal **que presta servicios por cuenta ajena** en la empresa y que, en virtud de las funciones y operaciones que tenga definidas en su perfil profesional, trate datos de carácter personal.

Respecto a los accesos del personal a los datos de carácter personal que trata la empresa como responsable del tratamiento, están restringidos y limitados a las personas autorizadas.

**CONSENTIMIENTO.**

La empresa trata los datos de carácter personal de sus empleados como consecuencia inevitable y necesaria de la relación laboral, y actuaría de forma engañosa si intentara legitimar este tratamiento a través del consentimiento. Por lo tanto **la empresa no basa el tratamiento de los datos de carácter personal de sus empleados en el consentimiento**, sino que emplea el contrato laboral como base jurídica.

**OBLIGACIONES.**

Lo establecido en este apartado es de aplicación al trabajador:

nombre y apellidos: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ DNI: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Departamento: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Cargo: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Centro de trabajo: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tiene concedidos los siguientes permisos:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nombramientos.

Se designa al trabajador como:

* ENCARGADO DE ASIGNACIÓN Y DISTRIBUCIÓN DE CONTRASEÑAS

*(El encargado de asignación y distribución de contraseñas es la persona designada por el Responsable del Tratamiento para llevar a cabo el control de los accesos a los datos de carácter personal, la gestión de las contraseñas para el acceso electrónico a los datos informatizados.)*

* ENCARGADO DE GESTIONAR EL REGISTRO DE INCIDENCIAS Y LAS VIOLACIONES DE SEGURIDAD.

*(El encargado de la gestión y registro de violaciones de seguridad es la persona designada por el Responsable del Tratamiento para llevar a cabo el registro y el control de las incidencias que se puedan producir con los datos de carácter personal como por ejemplo la pérdida de control de los datos, usurpación de identidad, daño para la reputación de los interesados, etc.. Estas incidencias ( y similares) son conocidas como VIOLACIONES DE LA SEGURIDAD DE LOS DATOS y la persona designada debe registrarlas, analizar las consecuencias, notificarlas si procede y en definitiva tomar las medidas oportunas siguiendo el procedimiento indicado por la empresa.*

* COORDINADOR DE SEGURIDAD y SALVAGUARDA.

*(El coordinador de seguridad y salvaguarda es la persona designada por el Responsable del Tratamiento para gestionar la protección de los datos recogidos de forma electrónica, implementando medidas técnicas, informáticas y organizativas que garanticen la salvaguarda de los datos, incluyendo el control de las copias de seguridad, el control de las entradas/salidas de los soportes electrónicos y la seguridad de los elementos informáticos (firewall, antivirus, etc..). Asimismo se encarga de verificar periódicamente si la protección tecnológica aplicada es adecuada y eficaz.)*

* ENCARGADO DE ATENDER LOS DERECHOS DE LOS USUARIOS.

*(El encargado de atender los derechos de los usuarios es la persona designada por el Responsable del Tratamiento para atender los derechos de los interesados, así como para gestionar y registrar cualquier petición que los interesados realicen ante el Responsable)*

**MEDIDAS ORGANIZATIVAS DE PROTECCIÓN DE DATOS.**

**Deber de confidencialidad y secreto.**

Debe evitar el acceso de personas no autorizadas a los datos personales, a tal fin evitará dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, procederá al bloqueo de la pantalla o al cierre de la sesión.

Los documentos en papel y soportes electrónicos se almacenan en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día. En caso de utilizar cualquier documento con datos de carácter personal debe devolver el documento a su archivo seguro.

Nunca desechar documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

No comunicar datos personales o cualquier información personal a terceros, prestando atención especial en no divulgar los datos protegidos durante las consultas telefónicas, correos electrónicos, etc.

**Derechos**

Cuando un interesado ejercite sus derechos lo pondrá en inmediato conocimiento del encargado de atender los derechos de los usuarios. El encargado, para la atención de los derechos de los interesados, tendrá en cuenta el siguiente procedimiento:

1.- Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos. Debe dar respuesta a los interesados sin dilación indebida.

2.- Debe registrar al peticionario en la aplicación de protección de datos.

3.- Debe entregar al interesado el documento justificativo de la solicitud formulada para su firma.

4.- Recibida la solicitud debe dar respuesta sin dilación indebida (como máximo un mes).

**Violaciones de seguridad.**

Cuando tenga conocimiento que se ha podido producir una violación de seguridad (como por ejemplo, el robo o acceso indebido a los datos personales) lo pondrá en inmediato conocimiento del encargado de las incidencias y violaciones de seguridad.

El encargado de atender las incidencias y brechas de seguridad deberá registrarla en la aplicación de protección de datos y notificarla a la AEPD.

**Videovigilancia**

En caso de que la empresa disponga de videograbadores, se informa que tienen finalidad de control laboral. Tendrá el derecho de acceso a las imágenes previa petición al responsable o al encargado designado. Se le solicitará una fotografía reciente y el Documento Nacional de Identidad. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestran imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se justificará convenientemente la existencia o no de imágenes del interesado.

**MEDIDAS TÉCNICAS DE PROTECCIÓN DE DATOS.**

**Identificación y acceso.**

Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal debe disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

El sistema de contraseñas seguras deberá contener un mínimo de 8 caracteres alfanuméricos, serán contraseñas irrepetibles, únicas e intransferibles.

Deberá modificar las contraseñas al menos con una frecuencia mensual, conservando un registro de los cambios así como de los usuarios que tienen acceso a los datos.

Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se debe disponer de un usuario y contraseña específicos (identificación inequívoca).

Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

Las contraseñas serán facilitadas por la persona encargada de la creación y asignación de contraseñas.

**Deber de salvaguarda.**

* **Actualización de ordenadores y dispositivos.** Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la medida de lo posible.
* **Malware**. En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales deberá asegurar que existe un sistema de **antivirus** que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
* **Cortafuegos o firewall.** Para evitar accesos remotos indebidos a los datos personales deberá garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
* **Cifrado de datos.** Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
* **Copia de seguridad**: Periódicamente realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que estén ubicados los datos, con el fin de permitir la recuperación de los mismos en caso de pérdida de la información.

**Entrada/Salida de soportes.** Debe mantener un control y un registro de entradas y salidas de los soportes que contienen datos de carácter personal. Los soportes en ningún caso podrán salir del centro de trabajo sin la autorización del coordinador.

No se deben vulnerar las medidas técnicas de protección de datos (actualizaciones, antivirus, firewall, cifrados, etc..) bajo ningún concepto.

**Uso de internet**

Los trabajadores son responsables de las sesiones iniciadas de Internet desde sus terminales de trabajo. Internet tiene carácter laboral, y no puede ni debe usarse con otros fines.

En ningún caso se pueden modificar las configuraciones de los navegadores del equipo, ni la activación de servidores o puertos sin autorización del coordinador de seguridad, o en su caso del responsable del tratamiento.

Debe evitarse la utilización de imágenes y sonidos distintos e incompatibles a la actividad laboral.

Se prohíbe expresamente el acceso y/o la descarga y/o el almacenamiento en cualquier soporte de páginas y contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres; de los formatos de imágenes, sonido o vídeo; de virus y códigos maliciosos y en general, todo tipo de programas sin la expresa autorización del coordinador de seguridad.

Queda vetada toda utilización ajena a las actividades de la empres, de los servicios de chat, foros u otros sitios similares. Tampoco se permite el acceso a páginas de juego en línea, o la descarga de cualquier dispositivo similar.

**Uso del sistema informático.**

Se prohíbe la instalación de cualquier programa o producto informático en el sistema de información, sin la correspondiente autorización del coordinador de seguridad o del responsable en su caso.

Las aplicaciones necesarias para el desempleo de su trabajo, serán instaladas exclusivamente por el coordinador de seguridad o del responsable en su caso.

No se permite la utilización de recursos del sistema informático puesto a disposición por la empresa con fines privados con cualquier otro fin diferente a los estrictamente laborales.

Se prohíbe revelar a persona alguna ajena a la empresa, información a la que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.

Se prohíbe facilitar a persona cualquiera ningún soporte conteniendo datos a los que hayan tenido acceso en el desempeño de sus funciones sin la debida autorización.

Se prohíbe utilizar cualquier información que hubiese podido ser obtenida por su condición de empleado de la compañía, con cualquier otro fin que no sea el estrictamente necesario para el desempeño de sus funciones.

**Uso del correo electrónico**

Los trabajadores son responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la empresa

Los empleados no deberán permitir la utilización de la cuenta y/o el correspondiente buzón a personas no autorizadas.

Los servicios de correo electrónico suministrados deben destinarse a uso estrictamente laboral.

Está prohibida la utilización, en los equipos provistos por la empresa, de buzones de correo electrónico de otros proveedores de Internet.

No es legal enviar correo a personas que no desean recibirlo. Si le solicitan detener esta práctica deberá hacerlo. Si la empresa recibe reclamaciones sobre esta práctica, se tomarán las medidas sancionadoras adecuadas.

Se prohíbe realizar cualquiera de las siguientes actividades:

* Utilizar el correo electrónico para cualquier propósito ajeno a las actividades laboral
* Participar en la propagación de cartas encadenadas, esquemas piramidales o similares.
* Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la empresa..
* Falsificar las cabeceras de correo electrónico.
* Recoger correo de buzones de otro proveedor de Internet.
* Difundir contenido ilegal o contrario a la moral y las buenas costumbres.
* Enviar correo propio a través de cuentas ajenas sin consentimiento de su titular.
* Efectuar ataques con objeto de imposibilitar u obstruir sistemas informáticos, dirigidos a un usuario o al propio sistema de correo, así como le envío de un número alto de mensajes por segundo, o cualquier variante que tenga por objeto la paralización del servicio por saturación de las líneas, de la capacidad de la CPU a del servidor, del espacio en disco de servidores, o terminales o cualquier otra práctica similar.
* Enviar a foros de discusión, listas de distribución o grupos de noticias, mensajes que comprometan la reputación de la empresa

**Propiedad intelectual**

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia así como el uso reproducción, cesión o transformación, o comunicación pública de cualquier tipo de programa informático protegido por los derechos de propiedad intelectual o industrial.

Se sancionará severamente a los trabajadores que lleven a cabo la instalación de tales programas, debido a que su acción podría ocasionar serias responsabilidades civiles y /o penales a la empresa.

El trabajador es responsable de los daños que pudiera derivarse por el incumplimiento de los compromisos anteriores, incluso después de extinguida la relación laboral.

**FIRMA, FECHA Y D.N.I DEL TRABAJADOR.**

**CONFORME RECIBIDO, LEÍDO Y ENTENDIDO.**