NORMATIVA PARA EL PERSONAL RELATIVA A PROTECCION DE DATOS, SEGURIDAD DE LA INFORMACION E INFORMATICA

Nombre Trabajador:

NIF trabajador:

ACCUAE SERVICIOS INTEGRALES S.L, ha implantado en la organización un sistema de gestión con el fin de garantizar los niveles de seguridad exigidos por la legislación vigente en materia de protección de datos de carácter personal.

Dentro de este proceso y como una parte fundamental del mismo está el respeto a la confidencialidad de sus datos personales, de los datos personales relativos al resto de la plantilla, de otros profesionales que no forman parte de la empresa y de los clientes y usuarios en general.

Con el fin de garantizar esta confidencialidad en el tratamiento de los datos personales de los trabajadores y de acuerdo con lo dispuesto en la ley de protección de datos personales y garantía de los derechos digitales y el Reglamento UE 679/2016, le informamos de que ACCUAE SERVICIOS INTEGRALES S.L, es responsable de ficheros en los que se tratan sus datos personales con la finalidad de realizar la gestión de nóminas, personal y recursos humanos, la formación y la prevención de riesgos laborales. Le informamos también de la existencia de controles de acceso a las instalaciones y de cámaras de Video vigilancia, instalados por seguridad y que pueden usarse con fines de control laboral, de conformidad, y con las limitaciones de los artículos 89 y 90 de la Ley Orgánica 3/2018 de 5 de Diciembre de Protección de datos Personales y Garantía de los derechos digitales.

Al mismo tiempo y en función de la relación laboral que el trabajador mantiene con ACCUAE SERVICIOS INTEGRALES S.L, y en la medida en la que en el ejercicio de sus funciones tiene o pueda tener acceso a datos de carácter personal y demás información confidencial relativa a clientes, a otros trabajadores, a proveedores y otros se pone en su conocimiento la obligación de confidencialidad respecto de los mismos, establecido en el art. 5.1.f del Reglamente UE 679/2016. Así como al deber de adoptar las obligaciones y deberes relativos al tratamiento de los datos personales en virtud de lo dispuesto en la normativa de protección de datos de carácter personal.

Se le informa también de la responsabilidad personal frente a terceros en la que pudiera incurrir a los efectos de resarcir los daños y perjuicios que se pudieran ocasionar derivados de un incumplimiento culpable, de las obligaciones en materia de protección de datos de carácter personal y otros confidenciales, propias de su puesto de trabajo y de que las obligaciones mencionadas subsistirán aun después de finalizar su relación de trabajo con ACCUAE SERVICIOS INTEGRALES S.L, de acuerdo con lo establecido en el art. 5.3 de la Ley Orgánica 3/2018 de 5 de Diciembre de Protección de datos Personales y Garantía de los derechos digitales.

El trabajador podrá ejercitar los derechos de acceso, rectificación, supresión, portabilidad y limitación de tratamiento de los datos que el conciernen dirigiendo escrito con copia de su DNI a la dirección de la empresa. También podrá en caso de no ver atendido sus derechos presentar reclamación ante la autoridad de control.

En particular el empleado cumplirá con las siguientes obligaciones tendentes a garantizar la seguridad de los sistemas informáticos y la integridad de los datos en ellos contenidos.

1.-Números de identificación, claves de acceso y uso y custodia de llaves

0.- Las contraseñas cumplirán los siguientes requerimientos (siempre que sea posible) para garantizar su complejidad:

No contener el nombre del usuario o partes del nombre de usuarios.

No pueden contener fechas relevantes en la vida del usuario ni información relevante para este. (fechas de cumpleaños, nombres de hijos etc)

Tener una longitud mínima de 6 caracteres.

Usar las combinaciones entre caracteres mayúsculas [A-Z], minúsculas [a-z] y números [0-9].

Caracteres no alfanuméricos (¡, #, $, %)

No tener contraseñas iguales enteras o parcialmente

1.- Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del responsable de seguridad con el fin de que le asigne una nueva clave.

2.- El usuario está obligado a utilizar la red corporativa y la Intranet de la entidad sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales o que infrinjan los derechos de la entidad, de los clientes o de terceros, o que puedan atentar contra la moral, la imagen de la entidad o las normas de cortesía.

3.- Están expresamente prohibidas las siguientes actividades:

-Compartir o facilitar el identificador de usuario y la clave de acceso facilitados por la entidad con otra persona.

-Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la entidad o de terceros. Estos actos podrían constituir un delito de daños previsto en el artículo 264.2 del Código penal.

-Enviar mensajes de correo electrónico de forma masiva sin que este hecho tenga relación con el desempeño del trabajo que tenga asignado.

-Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. Esta actividad podría constituir un delito de interceptación de las telecomunicaciones previsto en el artículo 197 del código penal.

-Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la entidad o de terceros.

-Introducir voluntariamente programas, virus, macros que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros.

-Introducir en su puesto de trabajo, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la entidad o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros cuando no se disponga de autorización para ello.

-Instalar copias ilegales de cualquier programa incluidos los estandarizados en su puesto de trabajo.

-Cambiar la configuración de los equipos sin autorización para ello.

-Borrar cualquiera de los programas instalados legalmente.

-Utilizar los recursos telemáticos de la entidad incluida la red Internet, para actividades que no estén relacionadas con el puesto de trabajo del usuario.

-Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la entidad en la red corporativa de la entidad.

4.- Uso y custodia de llaves:

Queda prohibido etiquetar las llaves con el nombre o dirección del cliente.

En el caso de pérdida de las mismas hay que informar a la empresa inmediatamente.

2.-Confidencialidad de la información

1.- Queda prohibido enviar/sacar información confidencial de la entidad al exterior mediante soportes materiales o a través de cualquier medio de comunicación. El trabajador impedirá incluso la simple visualización de cualquier tipo de documento o acceso no autorizado.

2.- Los usuarios de los sistemas de información corporativos deberán guardar por tiempo indefinido la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas los datos, documentos, metodologías, claves, análisis programas y demás información a la que tengan acceso durante su relación laboral con la entidad, tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato laboral.

3.- Ningún colaborador puede poseer para usos que no sean propios del desempeño de su puesto de trabajo ningún material o información propiedad de la entidad.

4.- En el caso de que por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información confidencial en cualquier tipo de soporte se entenderá que esta posesión es temporal con obligación de secreto y sin que ello le irrogue ningún derecho de titularidad o copia. Asimismo el trabajador deberá devolver dichos materiales a la entidad inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral.

3.- Uso del correo electrónico

1.- El sistema informático, la red corporativa y los terminales utilizados por cada usuario son propiedad de la entidad.

2.- Ningún mensaje de correo electrónico será considerado como privado. Todos los mensajes irán abiertos.

3.- La entidad se reserva el derecho a revisar sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa y de los archivos LOG del

servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la entidad como responsable civil subsidiario, todo ello respetando los artículos 87 y 88 de la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales.

4.-Se prohíbe el envío de mensajes en cadena o de tipo piramidal, se prohíbe la utilización del correo electrónico para todo tipo de fines particulares o no relacionados con la ejecución de tareas propias del puesto de trabajo.

4.-Acceso a Internet

1.- El uso del sistema informático de la entidad para acceder a redes públicas como Internet se limitará a los temas directamente relacionados con la actividad de la entidad y los cometidos del puesto de trabajo del usuario.

2.- El acceso a debates en tiempo real es especialmente peligroso ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema por lo que su uso queda estrictamente prohibido.

3.- El acceso a páginas web se limita a aquellas que contengan información relacionada con la actividad de la entidad y/o con los cometidos del puesto de trabajo del usuario.

4.- La entidad se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa, todo ello respetando los artículos 87 y 88 de la Ley 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.

5.- Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet deberá cumplir los requisitos establecidos en estas normas y en especial las referidas a propiedad intelectual e industrial y a control de virus.

5.- Incidencias

1.- Es obligación de todo el personal de la entidad comunicar al responsable de seguridad cualquier incidencia que se produzca en los sistemas de información a que tengan acceso.

2.- Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

3.- Dicha comunicación deberá realizarse inmediatamente.

6.-Uso de la telefonía

1.- Se prohíbe el uso de la telefonía de la entidad para fines privados, salvo autorización expresa. La recepción de llamadas particulares por el trabajador en el puesto de trabajo se limitará a aquellos casos graves y excepcionales, debiendo ser breve la extensión de las mismas.

2.- Si excepcionalmente se requiriese por parte del trabajador el uso particular de la telefonía de la entidad este deberá solicitar autorización expresa.

3.- El uso de los teléfonos móviles particulares durante la jornada laboral atenderá a motivos de urgencia y necesidad.

7.-Protección de datos

1.- Queda prohibido crear ficheros de datos personales sin la autorización del Responsable del Tratamiento.

2.- Queda prohibido cruzar información relativa a datos de diferentes ficheros o tratamientos, con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa de los responsables de la entidad.

3.- Queda prohibido cualquier otra actividad que ponga en peligro la seguridad de los datos personales recogido en este documento o en las normas sobre protección de datos o en el Registro de Actividades de Tratamiento.

8.-Política de Recursos tecnológicos

La entidad pone a disposición de sus trabajadores una serie de recursos tecnológicos (ordenadores, teléfonos móviles, portátiles, PDAs...) de los que el trabajador se compromete a hacer un uso profesional y responsable del mismo, quedando prohibido el uso personal de los mismos, sin autorización expresa de la entidad.

9.- Finalización o extinción de la relación laboral

A la finalización de la relación contractual laboral que une al trabajador con la entidad, este último deberá obligatoriamente proceder inmediatamente a la devolución de todos los recursos laborales puestos a su disposición para el desarrollo de sus funciones, tanto físicos (teléfonos móviles, PDA, tablets, ordenadores portátiles, discos duros, pendrive, listados en papel, contratos, formularios y cualquier otro documento en papel que contenga datos de carácter personal) como en soporte digital o informático (documentos Office, PDF, e-mails, archivos....) devolviéndolos al responsable junto con las copias de seguridad que haya hecho. Igualmente procederá al borrado de cualesquiera datos e información del ámbito doméstico o particular que hubiera podido almacenar en los citados recursos durante la prestación de sus servicios en la empresa.
El trabajador no podrá realizar ni almacenar fuera de la empresa copias de seguridad o documentación en papel propiedad de la entidad para la que trabaja sin el consentimiento expreso del responsable.

10.- Clausulas de no competencia

De conformidad con el artículo 21 del Estatuto de los Trabajadores, el trabajador se compromete a desarrollar su tarea profesional sin concurrencia desleal, quedando expresamente prohibido que el trabajador mantenga ninguna relación, sea ésta laboral o por cuenta ajena, con terceros que pudieran ser competencia, directa o indirecta, con la actividad llevada a cabo por el empleador.

El incumplimiento de lo anteriormente dispuesto facultará al empleador para proceder al despido disciplinario del trabajador, por incumplimiento grave de sus obligaciones contractuales. De igual forma, la compañía se reserva la posibilidad de sancionar al trabajador por los daños y perjuicios causados durante el tiempo que el trabajador hubiera incumplido el contrato.

El empleado se compromete a no extraer, almacenar, ceder o distribuir, de forma directa o indirecta, código fuente, código tipo, diagramas de flujo y, en definitiva, documentación relativa a sus labores desarrolladas bajo su relación laboral. En todo caso, el trabajador mantendrá la diligencia debida, responsabilizándose y

comprometiéndose en todo momento a garantizar la seguridad física y lógica de la información tratada en ejercicio de sus labores diarias.

11.- Consecuencias del incumplimiento de las obligaciones por parte de los trabajadores

-Administrativas: Sanciones económicas contempladas en la L Ley 3/2018 de 5 de Diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales y en el Reglamento UE 679/2016 e impuestas por la Agencia Española de Protección de Datos u otra autoridad de control.

-Laborales: Las consecuencias que se derivan del incumplimiento de las obligaciones por parte del trabajador, como son la protección inadecuada, la fuga de datos, el acceso no autorizado, etc. conlleva la puesta en marcha del poder disciplinario del empresario a través del despido y otras medidas disciplinarias de carácter laboral.

-Civiles: El incumplimiento de las obligaciones contractuales pueden estar relacionadas con los artículos 1902 y 1903 del Código Civil relativos a la Responsabilidad, según los cuales la entidad podrá ejercitar las acciones civiles que estime pertinentes para el posible resarcimiento en relación a daños y perjuicios que fruto de sus actos negligentes o malintencionados el trabajador pueda causar.

-Penales: El Código Penal tipifica los delitos contra la intimidad y el descubrimiento y revelación de secretos en los artículos 197 y siguientes, según los cuales la entidad podrá ejercitar las acciones penales que estime pertinentes para el posible resarcimiento y castigo de aquellos trabajadores que incumplan sus obligaciones y cuyos actos sean constitutivos de delito o faltas penalmente tipificados.

12.- Servicios de mensajería instantánea

El trabajador da su consentimiento para que la empresa realice comunicaciones a través de sistemas de mensajería instantánea (como WhatsApp etc.) así como para su inclusión en grupos de trabajo en estos mismos sistemas.

Y para que conste a los efectos oportunos, firma el trabajador que declara estar informado y recoge copia del presente documento.

En Pamplona a 27 de mayo de 2024