FUNCIONES Y OBLIGACIONES DEL PERSONAL O USUARIOS

Se considera usuario, a los efectos de la legislación aplicable en materia de protección de datos de carácter personal, el sujeto autorizado para acceder a datos de carácter personal o recursos que contienen datos de carácter personal.

Lo anterior expuesto supone que, aquella persona que por prestar sus servicios para **GESTIÓN DE RESIDUOS HUESCA, S.A.**, tenga autorizado el acceso a los ficheros contenidos en un Servidor Central, conectado en red a varios terminales y equipos portátiles y, en general, a cualquier dato de carácter personal facilitado por los afectados, quedará sujeto al control de su actividad por parte del Responsable de Seguridad, quien ha sido nombrado para ocupar el cargo y ejercer las facultades correspondientes a los Responsables de Seguridad. Así mismo, quedan inmediatamente obligadas a cumplir las prescripciones establecidas en el presente Documento conforme a la normativa reguladora de Protección de Datos de Carácter Personal, en cuanto a:

3.1. Confidencialidad de la información

3.2 Números de identificación y claves de acceso

3.3 Uso del correo electrónico

3.4 Acceso a Internet

3.5 Uso de programas de ordenador

3.6 Incidencias

3.7 Puestos de trabajo

3.8 Gestión de soportes

3.9 Otras medidas de seguridad interna

3.1. Confidencialidad de la información

Los usuarios tienen expresamente prohibido, mientras dure la relación de prestación de servicios para la empresa para la que desempeñan sus funciones laborales, así como una vez se haya extinguido la misma, comunicar procedimientos, información, datos financieros o comerciales, así como, trabajos encomendados por su empleador incluidos en las bases de datos y, en general, cualquier dato referido a los negocios o finanzas de **GESTIÓN DE RESIDUOS HUESCA, S.A.** y que hayan conocido tanto por razón de su trabajo en la empresa, como por cualquier otra causa.

Por este motivo, todos y cada uno de los empleados de **GESTIÓN DE RESIDUOS HUESCA, S.A.** habrán de firmar en el apartado designado para ello en el Documento de Seguridad, una vez les haya sido facilitado y hayan tenido ocasión de leerlo, informándose así de todas las obligaciones a las que quedan sujetos como consecuencia del tratamiento de datos de carácter personal que realizan en el cumplimiento de sus funciones.

Finalmente, todas las circulares, documentos, soportes informáticos, etc., que contengan datos de carácter personal relacionados con las actividades de la empresa, son propiedad de la misma; estando obligado todo trabajador, a devolverlos cuando así le sea solicitado por

GESTIÓN DE RESIDUOS HUESCA, S.A. y, en cualquier caso, con motivo de la extinción del contrato de trabajo.

Lo expuesto anteriormente supone que:

1) Queda absolutamente prohibida la utilización, divulgación o cesión de los datos de los afectados para finalidades diferentes a aquellas para las que hubieren sido facilitados.
2) Todo usuario autorizado para llevar a cabo el tratamiento de datos de carácter personal, queda obligado legalmente al secreto profesional respecto de los mismos, incluso una vez extinguida la relación laboral o de colaboración que le une con la empresa.
3) Queda absolutamente prohibido, revelar, permitir o facilitar el acceso a la información contenida en los ficheros de la empresa, sean autorizados o no, a terceras personas ajenas a la misma sin autorización del titular de dichos datos, así como a otros trabajadores de la empresa que, por sus funciones, no tengan autorizado el acceso a los datos de carácter personal.
4) Recopilar información acerca de otras personas, incluidas las direcciones de correo electrónico, sin su consentimiento.
5) Transmitir cualquier material que pueda infringir los derechos de propiedad intelectual u otros derechos, incluida la marca registrada o los derechos publicitarios.

En caso de plantearse dudas sobre el acceso a los datos de carácter personal de terceras personas, debe consultarse al Responsable de Seguridad o, en su caso, al Responsable del Fichero.

3.2 Números de identificación y claves de acceso

Los números de identificación y las claves de acceso serán proporcionados por el Responsable de Seguridad a cada uno de los usuarios de forma individualizada y tendrán carácter personal e intransferible, debido a lo cual, queda absolutamente prohibido comunicar a persona distinta del propio interesado, la clave de usuario y la contraseña (salvo autorización expresa del Responsable del Fichero o, en su caso, del Responsable de Seguridad).

Si el usuario tiene conocimiento de que otra persona conoce su clave y/o contraseña de identificación y acceso, deberá ponerlo inmediatamente en conocimiento del Responsable de Seguridad o, en su caso, del Responsable del Fichero, con el fin de que le sea asignada una nueva clave de usuario y contraseña de acceso y se proceda a cancelar la anterior. En caso de incumplimiento de esta obligación, el usuario será el único responsable de los actos realizados por la persona que utilice de forma no autorizada su identificador.

Lo expuesto anteriormente supone que está totalmente prohibido:

1. Intentar descifrar las claves, sistemas o algoritmos de cifrado usando métodos de desencripctación u otros.

2. Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas informáticos.

3. Intentar utilizar el sistema para acceder a áreas que el usuario tenga restringidas de los sistemas informáticos de la empresa o de terceros.
4. Intentar aumentar el nivel de privilegios de un usuario en el sistema.
5. Intentar acceder sin la debida autorización, al servidor, a otras cuentas o a sistemas de equipos o redes conectadas a Internet, a través del uso no lícito de la contraseña (o cualquier otro medio).

3.3 Normas de uso de correo electrónico

El sistema informático, la red interna y los terminales utilizados por los usuarios, son titularidad de **GESTIÓN DE RESIDUOS HUESCA, S.A.**. El correo electrónico tan sólo podrá ser utilizado, para llevar a cabo las tareas que sean encomendadas directamente a cada persona, sin que pueda en ningún caso, ser utilizado para fines particulares.
Cada usuario deberá, al menos, cumplir con las siguientes medidas:
1. El usuario deberá utilizar (siempre y cuando sea posible) métodos de cifrado que permitan el intercambio de información de forma confidencial, así como mecanismos fiables de autenticación.
2. Deberán reunir los mismos requisitos establecidos en el presente Documento de Seguridad todos los ficheros que se introduzcan en la red interna o en el terminal del usuario a través de correo electrónico.
3. Nunca se deberán abrir archivos adjuntos que provengan de un origen desconocido, ya que podrían contener lo que se conoce como “cartas bombas” o “virus”, que dañarían el sistema informático de la empresa.
4. Siempre se ha de cerrar la sesión de cada programa de correo una vez se haya terminado de utilizar el mismo. De esta forma, se puede impedir que intrusos no deseados tengan acceso a la cuenta de cada usuario.
5. No se ha de responder a mensajes no solicitados u otro tipo de correo ofensivo o de acoso. Respondiendo se confirma que se tiene una dirección de correo electrónico activa a la que se puede enviar constantemente correo electrónico no solicitado.

<u>Lo anteriormente expuesto supone que queda totalmente prohibido:</u>

1. Enviar mensajes de correo electrónico de forma masiva (spam) o con fines comerciales o publicitarios, sin el consentimiento ni del Responsable del Fichero, ni de los destinatarios de los mismos.
2. Intercalar correo electrónico de otros usuarios para intentar leerlo, borrarlo, copiarlo o modificarlo. Esta actividad puede constituir delito de interceptación de las telecomunicaciones, tipificado en el artículo 197 del Código Penal.
3. Queda terminantemente prohibido utilizar los equipos informáticos y las redes internas o externas de la empresa, para uso particular de los trabajadores y de las demás personas que colaboren con ella. En especial, queda prohibido recibir y enviar correo electrónico con mensajes o información particular o introducir contenidos obscenos, inmorales u ofensivos, de

acoso, difamatorios, abusivos, amenazadores, hirientes, vulgares y, en general, carentes de utilidad para los objetivos de la empresa.

4. Enviar o reenviar mensajes en cadena en la red corporativa de **GESTIÓN DE RESIDUOS HUESCA, S.A.** o redes externas, sin la debida autorización del Responsable de Seguridad.

3.4 Normas de acceso a Internet

El sistema informático y los terminales utilizados por los usuarios son titularidad de **GESTIÓN DE RESIDUOS HUESCA, S.A.**. Esta exclusiva titularidad permite a la empresa, comprobar de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada en la misma por cualquier usuario, cumpliendo en tales situaciones, las exigencias legales que legitiman dicha actividad.

El acceso a páginas Web, grupos de noticias, listas de distribución y otras fuentes de información del personal de la empresa, queda restringido a las materias estricta y directamente relacionadas con las funciones que desempeña cada trabajador dentro de la misma.

En las visitas a los diferentes servidores Web deben suministrarse únicamente los datos de carácter personal necesarios para hacer uso del servicio.

Con el objeto de evitar intromisiones indebidas, deben utilizarse los programas de navegación más actualizados y activar aquellas opciones que informen de la existencia de mecanismos ajenos que tienen como objetivo la obtención ilícita y no consentida de datos.

Lo anteriormente expuesto supone que queda totalmente prohibido:

1. Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos, sin autorización expresa por parte del Responsable del Fichero correspondiente, así como respecto de cualquier otro tipo de obra o material, cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización del Responsable de Seguridad.
2. Utilizar los recursos telemáticos de **GESTIÓN DE RESIDUOS HUESCA, S.A.** (incluidas las redes de Internet e Intranet) para actividades que no se hallen directamente relacionadas con el puesto de trabajo asignado a cada usuario.

3.5 Normas sobre el uso de los programas de ordenador

Únicamente podrán utilizarse aquellos programas de ordenador que hayan sido creados directamente por **GESTIÓN DE RESIDUOS HUESCA, S.A.** a través de cualquiera de sus empleados, para uso propio, o bien aquellos programas de ordenador de los que se haya obtenido la correspondiente licencia de uso por quien legalmente es titular de los derechos de explotación.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o inversión susceptible de protección por la normativa aplicable en materia de propiedad intelectual o industrial.

3.6 Incidencias

Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad e integridad de los datos de carácter personal, sistemas, soportes informáticos y archivos (estén automatizados o no).

Es obligación de todo el personal que preste sus servicios para **GESTIÓN DE RESIDUOS HUESCA, S.A.**, comunicar al Responsable de Seguridad cualquier incidencia que se produzca en los sistemas de información. Dicha comunicación deberá realizarse a la mayor brevedad posible desde el momento en el que se produce la incidencia o se tenga certeza de que pudiera producirse.

Toda incidencia (independientemente de la relevancia que tenga) debe ser puesta en conocimiento inmediato del Responsable de Seguridad de la empresa.

3.7 Puestos de trabajo:

a) Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

b) Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

c) Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

d) En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

e) Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el Libro de incidencias.

f) Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo al autorización del responsable de seguridad o por administradores autorizados del Anexo H.

3.8 Gestión de soportes

a) Los soportes que contengan datos del Fichero, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de

procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

b) Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

c) Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del Fichero que no estén por tanto relacionadas en el Anexo H.

3.9 Otras medidas de seguridad

Además de las medidas de política de seguridad interna expuestas anteriormente, también estará absolutamente prohibido:

1. Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de **GESTIÓN DE RESIDUOS HUESCA, S.A.** o de las bases de datos de terceros. Dichos actos pueden constituir un delito de daños, tipificado en el artículo 264.2 del Código Penal.
2. Introducir voluntariamente programas, virus, caballos troyanos, gusanos, bombas de relojería, robots de cancelación de noticias, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen, o sean susceptibles de causar, cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus establecidos en la empresa e implantados por el Responsable de Seguridad y estar al tanto de sus actualizaciones periódicas, para prevenir la entrada en el sistema informático de cualquier virus destinado a borrar o alterar los datos alojados en los sistemas informáticos implantados en la empresa.
3. Instalar copias ilegales de cualquier programa sin la correspondiente licencia preceptiva o sin la autorización del titular de los derechos de autor del mismo.
4. Desinstalar, eliminar o inutilizar cualquier programa que esté instalado legalmente en los sistemas informáticos de la empresa, sin la correspondiente autorización del Responsable de Seguridad.