# USUARIO AUTORIZADO-

# FECHA DE RETIRADA-

# FECHA DEVOLUCIÓN-

# DEFINICIÓN DE EQUIPOS Y SISTEMAS INFORMÁTICOS OBJETO DE TELETRABAJO

|  |  |  |  |
| --- | --- | --- | --- |
| **TIPO DE EQUIPAMIENTO** | **IDENTIFICATIVO** | **MARCA** | **UNIDADES** |
| [ ] PC SOBREMESA |  |  |  |
| [ ] PC PORTÁTIL  |  |  |  |
| [ ] PANTALLA  |  |  |  |
| [ ] IMPRESORA  |  |  |  |
| [ ] DISCO EXTERNO  |  |  |  |
| [ ] SMARTPHONE CON ACCESO A SISTEMAS Y UNIDADES DE RED |  |  |  |
| OTROS: |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# DEFINICIÓN DE SISTEMAS INFORMÁTICOS OBJETO DE TELETRABAJO

|  |  |  |
| --- | --- | --- |
| **SITEMA** | **DEFINICIÓN Y FUNCIONALIDAD DEL SISTEMA** | **PERMISOS** |
| Ej. Contabilidad | Ej. Sistema de gestión de facturación, contabilidad y cobros | Ej. Control total |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# DEFINICIÓN DE ARCHIVOS DOCUMENTALES OBJETO DE TELETRABAJO

|  |  |
| --- | --- |
| **ARCHIVO** | **DEFINICIÓN Y FUNCIONALIDAD** |
| Ej. Nóminas | Ej. Documentos de nóminas de trabajadores |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## El puesto de trabajo

Los puestos de trabajo (equipos informáticos y archivos documentales) estarán bajo la responsabilidad directa de cada uno de los usuarios, y bajo la supervisión y control del responsable de seguridad establecido por <SU RAZÓN SOCIAL O NOMBRE>.

## Almacenamiento de la información

<SU RAZÓN SOCIAL O NOMBRE>pone a disposición de los usuarios espacios para el almacenamiento de información de acuerdo con la política establecida. Los ficheros, documentos, bases de datos, etc. (automatizados o no) almacenados de acuerdo con la política vigente de <SU RAZÓN SOCIAL O NOMBRE>cuentan con un control de seguridad de acuerdo con las normativas vigentes.

No obstante, la información almacenada en lugar diferente del recomendado por la política de seguridad de <SU RAZÓN SOCIAL O NOMBRE>no contará con los estándares de seguridad obligatorios, quedando bajo la responsabilidad del usuario la aplicación de las medidas de seguridad.

# ACCESO A EQUIPOS Y SISTEMAS INFORMÁTICOS

## Acceso a la información

1. Acceder exclusivamente a la información a la que está autorizado.
2. Registrar como incidencia cualquier acceso no autorizado detectado a los datos personales.

## Uso de la cuenta de usuario y claves de acceso

El identificativo de usuario de <SU RAZÓN SOCIAL O NOMBRE>responsabiliza al propietario del mismo en cuanto a las acciones llevadas a cabo en los recursos de <SU RAZÓN SOCIAL O NOMBRE>.

<SU RAZÓN SOCIAL O NOMBRE>podrá auditar los registros generados por los movimientos llevados a cabo por todos los usuarios en los recursos de <SU RAZÓN SOCIAL O NOMBRE>. Cada acción o trabajo realizado sobre los archivos queda registrada por ficheros log de seguimiento.

Estos números y claves son personales e intransferibles. Será el usuario asignado a cada clave el responsable de la misma, respondiendo en su caso de las consecuencias derivadas de su cesión o pérdida.

El usuario deberá mantener una clave que no será descifrable fácilmente por terceros. Para su mantenimiento, la contraseña será renovada.

Queda terminantemente prohibido su cesión o comunicación a otra persona que no sea el responsable de la seguridad del fichero, en los casos que proceda.

Queda prohibido exponer los identificadores y claves en lugar visible o accesible a terceros. En caso de que se sospeche que otra persona conoce su clave de acceso, el usuario deberá promover el cambio de la misma, y comunicará estas circunstancias al responsable de seguridad.

El abandono de la sesión de usuario validada en cualquier puesto de trabajo está prohibida, y responsabiliza al propietario de la cuenta (identificativo). Por ello, es obligatorio bloquearla cuando se abandone el puesto de trabajo.

Queda prohibido el uso de estos identificadores en actividades que pudieran resultar ilícitas o ilegales, o que atentasen contra los derechos de los afectados o los principios constitucionales, así como contra <SU RAZÓN SOCIAL O NOMBRE>, tanto en imagen como en funcionamiento.

El responsable de la seguridad podrá solicitar dichos números y claves para el mantenimiento de un correcto funcionamiento de las medidas adoptadas por este documento, estando el usuario obligado a proporcionárselo. También podrá requerirlo en caso de ausencia temporal del usuario de sus labores en el tratamiento.

Se prohíbe terminantemente:

1. El acceso por cualquier medio a ficheros a los que no está autorizado.
2. El bloqueo de los ficheros y datos a los que tienen acceso otros usuarios, así como el cifrado de los mismos con el único fin de impedir otros tratamientos autorizados.
3. La manipulación caprichosa de los datos de carácter personal contenidos en los ficheros de <SU RAZÓN SOCIAL O NOMBRE>, así como la destrucción e inutilización de los mismos. Lo contenido en este punto puede ser constitutivo de delito según el artículo 264.2 del Código Penal.
4. La manipulación de la relación de usuarios y de autorizaciones.
5. La introducción en el sistema de <SU RAZÓN SOCIAL O NOMBRE>, programas o virus que afecten a la seguridad de los ficheros.
6. Cualquier otra actividad que altere el correcto funcionamiento de los sistemas de seguridad implantados por<SU RAZÓN SOCIAL O NOMBRE>.

## Uso adecuado de correo electrónico y acceso a Internet

1.- Utilizar las cuentas de correo únicamente con fines profesionales, de acuerdo a las funciones que por el puesto tiene asignada, quedando prohibido para uso privado y personal.

2.- No hacer uso de las cuentas para fines comerciales propios.

3.- No utilizar cuentas de correo de otros usuarios.

4.- Abstenerse de abrir o reenviar archivos de origen desconocido y/o dudosa procedencia.

5.- Usar un lenguaje apropiado en las comunicaciones, evitando expresiones groseras, que pudieran afectar al buen nombre de <SU RAZÓN SOCIAL O NOMBRE>.

6.- No acceder a páginas que por su contenido (pornográfico, xenófobo, etc) pudieran aceptar de manera negativa al buen nombre de 1413<SU RAZÓN SOCIAL O NOMBRE>.

7.- No enviar, ni reenviar correos con anexos pudieran contener información confidencial sin autorización de <SU RAZÓN SOCIAL O NOMBRE>y sin las debidas medidas de seguridad.

8.- No utilizar programas que no siendo de uso profesional, saturan el ancho de la banda de Internet.

<SU RAZÓN SOCIAL O NOMBRE>podrá llevar a cabo controles sobre accesos en Internet, tanto de manera rutinaria (con el fin de detectar irregularidades en el sistema), como en caso de que exista alguna sospecha fundada de alguna anomalía ya sea en el actuar del trabajador o en el funcionamiento del medio informático utilizado.

9.- <SU RAZÓN SOCIAL O NOMBRE>tendrá acceso al contenido de su correo profesional (cuentas de correo profesional que son propiedad de <SU RAZÓN SOCIAL O NOMBRE>en el caso de que usted abandone <SU RAZÓN SOCIAL O NOMBRE>y/o se ausente repentinamente, con el fin de que se pueda continuar con el trabajo diario. En el caso de que abandone <SU RAZÓN SOCIAL O NOMBRE>, sus correos serán eliminados del sistema.

# NORMATIVA RELACIONADA CON FICHEROS EN PAPEL

## Acceso a la información

1. Acceder exclusivamente a la información a la que está autorizado.
2. Registrar como incidencia cualquier acceso no autorizado detectado a los datos personales.

## Uso de ficheros o copias de documentos con carácter temporal

1. Eliminar de forma confidencial los ficheros o copias temporales de documentos para el trabajo diario. Garantizar la confidencialidad e integridad de estos archivos o copias temporales de documento.

## Desecho y reutilización de soportes

1. Garantizar que no existen datos personales contenidos en el soporte a reutilizar (documentos de reciclaje).
2. Aplicar medidas que impidan la recuperación posterior indebida de la información contenida en el soporte a desechar (destrucción de documentos).

# CLÁUSULA DE CONFIDENCIALIDAD Y SECRETO PROFESIONAL

El trabajador se compromete de manera expresa, tanto durante la vigencia de la situación de teletrabajo, como después de su finalización, a no difundir, transmitir, revelar a terceras personas cualquier información de <SU RAZÓN SOCIAL O NOMBRE> a la que tenga acceso como consecuencia del desempeño de su actividad laboral, ni a utilizar tal información en interés propio o de sus familiares o amigos.

La prohibición establecida en el párrafo anterior se extiende a la reproducción en cualquier soporte de la información de la empresa  <SU RAZÓN SOCIAL O NOMBRE> a la que tenga acceso sobre clientes, procedimientos y sistemas de organización, programas informáticos o cualquier otro tipo de información interna, salvo que tal información sea estrictamente necesaria para el desarrollo del contenido inherente de su puesto de trabajo y se realice dentro del ámbito de la empresa.

Todas las notas, informes y cualesquiera otros documentos (incluyendo los almacenados en dispositivos informáticos), elaborados por el trabajador durante el periodo de teletrabajo y que se refieran a la actividad de la empresa son propiedad de <SU RAZÓN SOCIAL O NOMBRE> y serán diligentemente custodiados en la empresa.

En el supuesto de incumplimiento del compromiso asumido y con independencia de la extinción del contrato, <SU RAZÓN SOCIAL O NOMBRE>, se reserva el derecho de reclamar el resarcimiento de los daños y perjuicios que le pudieran causar como consecuencia de la vulneración del deber de confidencialidad y secreto profesional pactado en la presente cláusula.

En cumplimiento **principio de responsabilidad activa** establecido por el Reglamento General de Protección de Datos de la Unión Europea y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales , se ha informado al trabajador.

|  |
| --- |
| *firma* |
| *nombre*  | *dni* |