|  |
| --- |
| **CREDENCIAL DE USUARIO DEL CLIENTE DE LA PAI** |

|  |  |
| --- | --- |
| **Apellidos y nombre del usuario** | **NIF** |
|  |  |

*\* El nombre y apellidos deben escribirse tal como aparecen en el DNI/NIF/NIE/TIE.*

Declara que ha sido informado sobre sus responsabilidades respecto al tratamiento de datos de carácter personal y se compromete a cumplir todas las normas de seguridad relativas al uso de los medios informáticos y telemáticos, que conforman el Sistema de Información **PLATAFORMA AUTONÓMICA DE INTEROPERABILIDAD PAI),** según está previsto y fijado en el Alta de Usuario.

Las obligaciones del Usuario, recogidas en el reverso del presente documento, se articulan en cumplimiento de la legislación estatal y autonómica:

* Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 07/12/2018),
* Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
* Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica,
* Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica,
* Decreto 220/2014, de 12 de diciembre de 2014, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana,
* DECRETO 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat,
* DECRETO 130/2012, de 24 de agosto, del Consell, por el que se establece la organización de la seguridad de la información de la Generalitat,

Las citadas obligaciones podrán ser objeto de modificaciones, en orden a los cambios legislativos, tecnológicos, de organización o funcionamiento de la entidad pública.

Los datos de carácter personal contenidos en el impreso podrán ser incluidos en un fichero para su tratamiento por este órgano administrativo, como titular responsable del fichero, en el uso de las funciones propias que tiene atribuidas y en el ámbito de sus competencias. Así mismo, se le informa de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

**(i) Clave de acceso al sistema informático.-** La contraseña de acceso al sistema informático es personal e intransferible, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Queda prohibido, asimismo, emplear identificadores y contraseñas de otros Usuarios para acceder al sistema informático. La contraseña debe memorizarse, estando prohibido anotarla en lugares visibles o guardarla en lugares accesibles. Se cambiará con la periodicidad marcada por la política de la organización.

**(ii) Bloqueo o apagado del equipo informático.-** Bloquear la sesión del Usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático.

**(iii) Almacenamiento de archivos o ficheros en la red informática.-** Guardar todos los ficheros de carácter personal empleados por el Usuario, en el espacio de la red informática habilitado, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.

**(iv)** **Manipulación de los archivos o ficheros informáticos.-** Únicamente las personas autorizadas, podrán introducir, modificar o anular los datos personales contenidos en los ficheros. En el caso de que cualquier Usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del responsable del PAI.

**(v)** **Generación de ficheros de carácter temporal.-** Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s. Estos ficheros deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática.

**(vi)** **No uso del correo electrónico para envíos de información de carácter personal sensible.-** No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

**(vii)** **Comunicación de incidencias que afecten a la seguridad de la información.-** Comunicar al Centro de Atención al Usuario las incidencias de seguridad de las que tenga conocimiento, que puedan afectar a la seguridad de la información. Entre otros, tienen la consideración de **incidencia** de seguridad que afecta a los ficheros informáticos, los sucesos siguientes: pérdida de contraseñas de acceso a los Sistemas de Información, uso indebido de contraseñas, acceso no autorizado de usuarios a ficheros excediendo sus perfiles, pérdida de soportes informáticos con datos de carácter personal, pérdida de datos por mal uso de las aplicaciones, ataques a la red, infección de los sistemas de información por virus u otros elementos dañinos, fallo o caída de los Sistemas de Información, etc.

|  |
| --- |
| *Fecha:* |
| *Firma del usuario:* |