



Acuerdo de confidencialidad y tratamiento de datos de carácter personal usuario externo

D./Dña. _____ con DNI nº _____, en adelante el USUARIO EXTERNO, en virtud de la autorización para acceder a los Sistemas de Información de Asepeyo Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social nº151, en adelante ASEPEYO, se compromete al cumplimiento de los siguientes pactos:

1. El USUARIO EXTERNO, al amparo de la prestación del servicio establecida con ASEPEYO, en adelante EL SERVICIO, tiene acceso a información confidencial propiedad de ASEPEYO.
2. Se considera información confidencial, en adelante INFORMACIÓN CONFIDENCIAL, cualesquiera tipos de datos, datos personales, documentos, metodologías, identificaciones, claves, programas y demás información a la que tenga acceso para la prestación del SERVICIO en cualquiera de los soportes en que ésta resida.
3. El USUARIO EXTERNO se compromete a guardar de forma indefinida la máxima reserva y a no divulgar, utilizar, ni publicar directamente ni a través de terceras personas o empresas la INFORMACIÓN CONFIDENCIAL. Dicha información solo podrá ser utilizada para las finalidades propias DEL SERVICIO prestado. La utilización de la INFORMACIÓN CONFIDENCIAL en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de ASEPEYO no supone, en ningún caso, una modificación de este pacto y será responsabilidad DEL USUARIO EXTERNO.
4. De igual modo, el USUARIO EXTERNO se compromete a comunicar de inmediato, y de forma fehaciente a ASEPEYO la finalización, por cualquier causa, de la prestación del SERVICIO. Tras la finalización DEL SERVICIO, el USUARIO EXTERNO se compromete a no conservar en ningún tipo de soporte copia alguna de la INFORMACIÓN CONFIDENCIAL, así como devolver dichos materiales inmediatamente a ASEPEYO.
5. El incumplimiento por parte del USUARIO EXTERNO de cualquiera de las obligaciones establecidas en el presente acuerdo, dará derecho a ASEPEYO a reclamar una indemnización por los daños y perjuicios que le sean causados.
6. El USUARIO EXTERNO asume que toda la información existente en la Red Corporativa y/o aplicaciones es propiedad de ASEPEYO, siendo de uso exclusivo para la prestación DEL SERVICIO. Asimismo, en el caso de que el USUARIO EXTERNO disponga de una cuenta de correo electrónico corporativa de ASEPEYO, éste autoriza expresamente a ASEPEYO a acceder a los mensajes de su cuenta con el fin de posibilitar la debida continuación de la actividad de la empresa en los periodos de baja (temporal o definitiva) o vacacionales del USUARIO EXTERNO.
7. El USUARIO EXTERNO declara conocer la "Política de Seguridad" de ASEPEYO que figura en el reverso presente acuerdo. Ésta es de obligado respeto y cumplimiento por parte del USUARIO EXTERNO. Asimismo se compromete expresamente a adoptar cuantas medidas de seguridad fuesen necesarias para asegurar la confidencialidad, disponibilidad, secreto e integridad de la INFORMACIÓN CONFIDENCIAL a la que tiene acceso.

Asimismo, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, ASEPEYO informa al USUARIO EXTERNO que sus datos de carácter personal serán incorporados a un fichero debidamente inscrito en la Agencia Española de Protección de Datos. La finalidad del mismo es la adecuada gestión y control de acceso a los sistemas de información de esta Mutua. Los datos facilitados únicamente podrán ser comunicados a terceros expresamente autorizados o aquellos que colaboren directamente en el cumplimiento de la finalidad antes indicada, y siempre de acuerdo a los requerimientos que legalmente sean exigibles.

Adicionalmente, ASEPEYO informa al USUARIO EXTERNO que tiene derecho a la consulta, rectificación, cancelación y oposición de sus datos pudiéndolos ejercitar mediante solicitud dirigida a ASEPEYO, c/ Vía Augusta nº 36, 08006 Barcelona, a través del correo electrónico a la dirección asepeyo@asepeyo.es, contactando con nuestro servicio de atención al usuario (902 151 002) y/o personándose en uno de nuestros centros asistenciales.

En prueba de conformidad de cuantos apartados integran el presente acuerdo, EL USUARIO EXTERNO lo suscribe y firma en _____, a _____, de _____ de _____

Firmado: D./Dña



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE ASEPEYO

Identificación y autenticación del personal autorizado

- El acceso a los Sistemas de Información de ASEPEYO se efectúa mediante un Identificador de Usuario y una Contraseña. Todos los Usuarios de los Sistemas de Información de ASEPEYO deben identificarse en el momento de acceder al mismo.
- El Identificador de Usuario es único, y está asociado a la correspondiente Contraseña que sólo es conocida por el propio Usuario.
- Las acciones que se realizan en la Red Corporativa de ASEPEYO son registradas y monitorizadas a partir de los ficheros LOG de los servidores y aplicaciones. El uso del Identificador de Usuario y la Contraseña asignados implica la aceptación, como documento probatorio de la acción efectuada, de los registros generados en dichos archivos LOG y almacenados en los Sistemas de Información.

Salvaguarda y protección de las Contraseñas personales

- Los Identificadores de Usuario y Contraseñas de acceso asignadas a cada Usuario, son personales e intransferibles. El Usuario es el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o falta de diligencia respecto a las credenciales de acceso.
- Cada Usuario es responsable de la confidencialidad de su Contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, debe registrarlo como incidencia y proceder inmediatamente a su cambio.
- No está permitido compartir o facilitar el Identificador de Usuario y la Contraseña facilitados por ASEPEYO con otra persona, incluido el personal de ASEPEYO.

Control de acceso a datos y recursos

- Toda la información residente en la Red Corporativa de ASEPEYO, de forma estática o circulando por ella, es propiedad de ASEPEYO y tiene el carácter de confidencial.
- Tienen el carácter de información especialmente confidencial:
 - los datos de carácter personal que la LOPD clasifica como nivel medio y alto (sanitarios, prestaciones, mutualistas, sindicales, etc.)
 - los datos internos de la actividad de ASEPEYO que no son públicos
 - las estrategias, políticas, métodos, procedimientos y en general cualquier normativa interna de ASEPEYO
- Cada Usuario tiene unos privilegios asociados a su perfil, en función de los cuales puede acceder únicamente a aquellos datos y funciones que precise para el desarrollo de sus funciones.

Equipos informáticos

- El Sistema de Información, la Red corporativa y los equipos y datos utilizados son propiedad de ASEPEYO.
- Cada ordenador dispone de un protector de pantalla con Contraseña, que se activa manualmente mediante la función Inicio/Bloquear Estación o bien pulsando simplemente la tecla F11. Se debe utilizar esta función siempre que se ausente de su puesto de trabajo y quede por tanto el equipo, fuera de su control o accesible a otras personas.
- En el caso de las impresoras se debe asegurar que no quedan documentos impresos en la bandeja de salida.
- Se debe apagar el equipo de su puesto de trabajo (Inicio\Apagar el sistema) al finalizar su jornada laboral o en previsión de una inactividad prolongada.

Incidencias de seguridad

- Se debe comunicar de forma fehaciente y a la mayor brevedad, cualquier incidencia que se produzca en los Sistemas de Información a los que tenga acceso y que afecte o pueda afectar a los datos.
- El conocimiento y la no notificación de una incidencia se considera como una falta contra la seguridad de los Ficheros.

Tratamiento de la documentación/soportes

- Para prevenir la exposición al robo de información y de recursos de tratamiento de datos durante las ausencias de su puesto de trabajo, toda la documentación debe quedar fuera del alcance de personal no autorizado y en lugares de acceso restringido.
- Los Usuarios del Sistema de Información deben 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, Contraseñas, análisis, programas y demás información a la que tengan acceso durante su relación laboral con ASEPEYO, tanto en soporte material como electrónico.
- Los documentos de carácter confidencial serán enviados en sobres cerrados indicando tal circunstancia.
- Bajo ningún concepto se permite facilitar ningún dato de carácter personal a personas pertenecientes y/o externas a ASEPEYO, a excepción de aquellos casos necesarios para el desempeño de las funciones propias.
- Toda documentación que contenga información confidencial debe ser almacenada en estancias dedicadas, aisladas del resto de la documentación, y permanentemente cerradas con llave o otros mecanismos de control físico. El acceso a estas estancias está restringido única y exclusivamente a aquellas personas que así lo requieren para el desempeño de sus funciones.
- Toda documentación que contenga información confidencial debe destruirse en un destructor de documentos antes de su eliminación, o bien, depositarse en un recipiente adecuado, para su posterior destrucción (reciclaje).
- Las copias, duplicados, reproducciones, etc. de este tipo de documentación debe limitarse a aquellos casos imprescindibles.
- El resto de documentación, cuyo contenido no sea considerado como confidencial, puede ser depositada en los contenedores de reciclaje de papel. Debe evitarse la destrucción manual de cualquier documento.
- Encima de la mesa de trabajo debe existir la documentación mínima e imprescindible para la actividad diaria (especialmente en aquellos puestos en los que se atiende a personas ajenas a la mutua). Es conveniente que la documentación esté clasificada en carpetas que eviten, de forma accidental o intencionada, la visualización de ésta por parte de terceros.
- Al finalizar la jornada laboral, la documentación confidencial debe permanecer debidamente custodiada ya sea en archivadores propios o en aquellos de uso compartido por todo el centro. En ambos casos, los archivadores deberán permanecer cerrados con llave.
- Durante el traslado de documentación de un lugar a otro se debe garantizar la confidencialidad de la misma. A tal efecto se utilizarán carpetas opacas, sobres, etc. que impidan ver los documentos de su interior.
- Cualquier acceso a documentación especialmente protegida debe quedar convenientemente registrado, adjuntando una hoja con un registro manual en el interior de las carpetas que contienen esta clase de documentación.
- Los soportes de almacenamiento (CD, DVD, tarjetas de memoria) no deben tirarse directamente a papeleras, contenedores, etc. Siempre que sea posible es conveniente borrar la información que contienen o inutilizarlos (p.e. rallando ambas superficies en el caso de CD, DVD).

Internet y correo electrónico

- La utilización del Correo Electrónico se limitará a los temas directamente relacionados con la actividad de ASEPEYO y las funciones del puesto de trabajo.
- Las cuentas de Correo Electrónico son personales e intransferibles. El Usuario es responsable de todas las actividades que se realicen con su cuenta de Correo Electrónico.
- ASEPEYO se reserva el derecho de revisar, sin previo aviso, los mensajes de Correo electrónico de la Red Corporativa y los archivos LOG del servidor, para identificar situaciones irregulares.
- No está permitido el envío de mensajes de Correo Electrónico de forma masiva o con fines comerciales o publicitarios (spam), ni el redireccionamiento automático de correos electrónicos a otras cuentas de correo externas.
- El uso de Internet se limitará, salvo en el caso de que se cuente con autorización para lo contrario, a los temas directamente relacionados con la actividad de ASEPEYO y las funciones del puesto de trabajo.