CONFIDENCIALIDAD, NORMATIVA DE USO DE SISTEMAS Y FUNCIONES DEL PERSONAL EXTERNO

1. CONFIDENCIALIDAD

La prestación de servicios por personal empleado por terceros proveedores de servicios, (en adelante, el "**Usuario"**), podrá implicar el acceso a información del **Grupo Hospitalario Quirónsalud** considerada como confidencial.

Toda información a la que se tenga acceso como consecuencia de la prestación de los servicios del Usuario, será considerada como confidencial y no podrá ser divulgada, mostrada, reproducida, copiada, discutida con terceros, ni empleada para fines ajenos al servicio, sin la previa conformidad por escrito del **Grupo Hospitalario Quirónsalud**.

Se entiende por información confidencial, toda la información relativa al **Grupo Hospitalario Quirónsalud**, sus sociedades, de carácter técnico, económico, de negocio o comercial así como cualquier documento, método, experiencia o know how adquirido y en general cualquier información concerniente o relativa al **Grupo Hospitalario Quirónsalud** y que no sea de dominio público.

Este compromiso de confidencialidad deberá mantenerse durante la vigencia de la prestación del servicio, así como con posterioridad a la terminación del mismo.

2. NORMATIVA INTERNA DE USO DE SISTEMAS DE LA INFORMACIÓN

La prestación de los servicios que implique el uso de aplicaciones informáticas, correo electrónico, Internet y otros recursos tanto software como hardware, (en adelante, los "**Recursos**") facilitados por el **Grupo Hospitalario Quirónsalud** para el desarrollo de las funciones propias del servicio, requerirá la atención de las siguientes normas de obligado cumplimiento:

- El uso de los Recursos queda limitado a fines estrictamente profesionales y relacionados con las funciones propias del puesto de trabajo.
- No se almacenará en la memoria de los ordenadores documentos que contengan datos personales.
- Todo Usuario deberá utilizar los Recursos de forma diligente, sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de terceros o que puedan atentar contra la moral o las normas de buen uso de las redes telemáticas.
- El Usuario deberá notificar cualquier incidencia que detecte en relación al incorrecto funcionamiento de los sistemas, así como en aquellos procesos que afecten al tratamiento de datos personales.
- No está permitido: proporcionar a otras personas la contraseña a los diferentes Recursos; dejar la clave de forma visible en lugares o documentos en los que pueda ser vista por terceros; hacer uso de claves de terceros, independientemente del método utilizado para su obtención; utilizar para fines privados los Recursos; obstaculizar voluntariamente el acceso de otros usuarios al sistema informático del **Grupo Hospitalario Quirónsalud** mediante el consumo masivo de los Recursos, así como realizar acciones que dañen, interrumpan o generen errores en dicho sistema; introducir voluntariamente programas, virus, macros, applets o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en el sistema del **Grupo Hospitalario Quirónsalud**; descargar de Internet, reproducir, utilizar, ceder, transformar, comunicar públicamente o distribuir documentos o programas informáticos no autorizados expresamente 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; utilizar los Recursos para descargar o instalar copias ilegales de cualquier programa, incluidos los estandarizados; utilizar los Recursos titularidad del **Grupo Hospitalario Quirónsalud**, puestos a su disposición, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el desarrollo de las funciones profesionales.

El **Grupo Hospitalario Quirónsalud** se reserva el derecho de poder revisar los mensajes de correo electrónico y monitorizar cualquier sesión de acceso a Internet con el fin de comprobar el cumplimiento de las normas recogidas en el presente documento, así como el cumplimiento y respeto de lo dispuesto en ***CORP6.5/P1 Procedimiento de seguridad de uso de los sistemas de información*** disponible en la Intranet. A tal efecto, el Usuario queda informado y consiente expresamente que tanto los mensajes de correo electrónico así como el acceso a internet a través de los Recursos facilitados puedan ser objeto de monitorización y revisión.

3. FUNCIONES Y OBLIGACIONES EN EL TRATAMIENTO DE DATOS PERSONALES

Se entiende por "dato personal" toda información sobre una persona físicas identificada o identificable.

El Usuario sólo tratará los datos personales necesarios para el desempeño de las funciones que le sean asignadas y exclusivamente para el cumplimiento de las mismas, quedando prohibido su uso para fines distintos.

El Usuario debe tratar los datos personales de modo que no puedan ser conocidos por usuarios no autorizados o terceros, salvo que, para cumplimiento de las funciones asignadas, así se le autorice.

El Usuario se compromete al efectivo cumplimiento de las presentes medidas de seguridad en el desempeño de sus funciones.

El Responsable del Tratamiento se reserva el derecho a exigir las responsabilidades que puedan derivarse del incumplimiento por el Usuario de las mismas.

El Usuario debe cumplir las medidas de seguridad señaladas en el siguiente cuadro:

a) Gestión de Soportes

- Los soportes y documentos que contengan Datos personales deberán permitir identificar el tipo de información que contienen y ser inventariados.

- El Usuario está autorizado para la entrada y salida de soportes o documentos fuera de los locales del responsable, incluidos los comprendidos y/o anejos a un correo electrónico, que contengan datos personales meramente identificativos (Nombre, apellidos, número de DNI o domicilio, por ejemplo) siempre que en el traslado adopte las medidas de seguridad razonables, dirigidas a evitar la sustracción, pérdida, manipulación o acceso por terceros a la información(envío en sobre cerrado, protección con llave/contraseña o custodia personal, por ejemplo).

- Cuando los soportes o documentos, incluidos los comprendidos y/o anejos a un correo electrónico contengan datos personales su entrada y salida deberá realizarse por cauces que permitan su adecuado registro (a través del correo postal centralizado o correo electrónico cifrado corporativo, por ejemplo), en otro caso, el usuario deberá solicitar autorización.

- El Usuario al que se haga entrega de dispositivos portátiles que así lo permitan, podrá proceder al tratamiento de Datos Personales fuera de los locales. Esta autorización regirá durante el tiempo que el dispositivo portátil se mantenga a su disposición, siempre que no se le informe en contrario.

Nombre y Apellidos:	**DNI:**
Fecha:	**Firma:**

CONFIDENCIALIDAD, NORMATIVA DE USO DE SISTEMAS Y FUNCIONES DEL PERSONAL EXTERNO

- A la hora de desechar un soporte o documento que contenga datos personales, el Usuario deberá destruirlo o borrarlo de modo que se impida el acceso a la información contenida en el mismo o su recuperación posterior. Si el soporte o documento es el único en que se contienen los Datos personales, el usuario deberá solicitar autorización previa a su destrucción o borrado.

- El Usuario deberá devolver todos los soportes y documentos a los que tenga acceso después de la finalización de las tareas que hayan originado su uso y, en cualquier caso, a la finalización de la relación contractual.

- El archivo de los soportes o documentos que contengan Datos personales se realizará de modo que garantice su correcta conservación, localización y la consulta de la información que contengan, de acuerdo con los criterios seguidos en el departamento al que pertenezca el usuario. Su archivo con criterios distintos deberá ser comunicado y autorizado.

- El Usuario conservará los soportes o documentos en los dispositivos de almacenamiento facilitados al efecto, en zonas que no permitan el acceso de terceros y adoptando medidas que impidan su visualización por usuarios no autorizados. En la medida de lo posible y en función de su contenido, se almacenarán en dispositivos que obstaculicen su apertura.

- Mientras los soportes o documentos con datos personales no se encuentren archivados, el Usuario deberá custodiarlos e impedir en todo momento que puedan ser accedidos por terceros o usuarios no autorizados (por ejemplo, retirar los documentos de la impresora antes de que puedan ser accedidos por usuarios no autorizados, o dejar su puesto de trabajo en un estado que impida la visualización de Datos personales cuando lo abandone).

b) Ficheros Temporales

- El Usuario no creará ficheros temporales o copias de documentos (creados para un tratamiento ocasional o como paso intermedio durante la realización de otro tratamiento) salvo que resulte estrictamente necesario para el desarrollo de sus funciones. En ese caso, el usuario deberá aplicar sobre los ficheros temporales o copias de documentos creados las mismas medidas de seguridad que correspondan a los Ficheros o documentos originales.

- El Usuario deberá mantener los datos registrados en los ficheros temporales o copias de documentos permanentemente actualizados.
- Una vez que hayan dejado de ser necesarios para los fines que motivaron su creación, el Usuario deberá proceder a su borrado o destrucción contraseñas

c) Contraseñas

- El Usuario debe proteger la confidencialidad de las contraseñas que se le asignen y es responsable de su custodia. Si tiene conocimiento de que las mismas son conocidas por personas no autorizadas, tendrá que comunicarlo como incidencia y solicitar el cambio de las mismas.

- El Usuario deberá cambiar las contraseñas cada vez que caduquen o así se le indique.

d) Gestión de incidencias

- El Usuario deberá comunicar aquellas incidencias de las que tenga conocimiento de forma inmediata (como máximo en las 8 horas siguientes), para la correcta gestión de las mismas. Si no lo hiciera, se considerará como una falta del Usuario contra la seguridad de los datos personales. Salvo que se le informe de la existencia de un sistema específico para la gestión de este tipo de incidencias, el Usuario las comunicará mediante el sistema general, indicando la afectación a Datos Personales.

e) Equipos o puestos de trabajo

- El Usuario tiene prohibido modificar la configuración de los equipos o puestos de trabajo desde los que pueda acceder a Datos personales salvo autorización expresa.

f) Confidencialidad

- El Usuario deberá observar el deber de secreto profesional respecto de los Datos personales de los que tenga conocimiento, manteniendo absoluta confidencialidad y reserva sobre los mismos.

- Esta obligación continuará vigente tras la terminación de la relación laboral, con carácter indefinido.

g) Tratamiento de categorías especiales de datos personales (si aplica)

Son categorías especiales de datos personales las relativas a origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos, datos relativos a la salud, vida sexual u orientación sexual de una persona física.

- El acceso a estas categorías de datos personales queda registrado y puede ser objeto de auditoría de acceso.

- Para la transmisión de datos personales a través de redes públicas o redes inalámbricas de comunicaciones electrónicas, o para su para su tratamiento fuera de los locales en dispositivos portátiles, el Usuario deberá solicitar el cifrado previo de dichos datos.

- El Usuario deberá almacenar los datos personales en armarios, archivadores u otros elementos que se encuentren en áreas cerradas, en las que el acceso esté protegido con puertas bajo llave o dispositivo equivalente, impidiendo el acceso por terceros o usuarios no autorizados.

- El Usuario utilizará un sistema de identificación de soportes y documentos que contengan datos personales que dificulte su comprensión a usuarios no autorizados o terceros, de acuerdo con los criterios seguidos en el departamento al que pertenezca el usuario.

- El Usuario deberá supervisar la generación de copias o la reproducción de los documentos bajo su custodia que contengan datos especialmente protegidos.

La violación grave o continuada de este documento o de lo dispuesto en el ***CORP6.5/P1 Procedimiento de Seguridad de Uso de los Sistemas de Información*** disponible en la Intranet, o abuso del sistema podrá repercutir en la terminación de privilegios de uso de los sistemas de información y pueden ser referidos al responsable correspondiente para la adopción de las medidas pertinentes.

Nombre y Apellidos:	**DNI:**
Fecha:	**Firma:**