Dirección General de Sistemas
de Información y Equipamientos Sanitarios
SERVICIO MADRILEÑO DE SALUD
CONSEJERÍA DE SANIDAD

FORMULARIO DE ACCESO A LOS SISTEMAS DE INFORMACIÓN DE ATENCIÓN PRIMARIA GAR_ASISTENCIAL-AP

MODALIDADES DE ACCESO A LOS SISTEMAS DE INFORMACIÓN DE ATENCIÓN PRIMARIA POR PARTE DEL GRUPO GAR_ASISTENCIAL-AP E INSTRUCCIONES PARA LA CUMPLIMENTACIÓN DEL FORMULARIO

El presente documento, recoge el formulario de solicitud de acceso a los sistemas de información de Atención Primaria por parte del Grupo de trabajo considerado GAR_ASISTENCIAL-AP. Dentro de esta GRUPO quedan incluidos los profesionales que se encuentran trabajando en las nuevas Unidades de Atención en las Residencias sociosanitarias (UAR), así como el personal de atención domiciliaria. Las personas encuadradas dentro de este grupo podrán tener acceso, a través de VPN a la aplicación AP Madrid dentro de su horario laboral.

En este sentido, la Dirección General de Sistemas de Información y Equipamientos Sanitarios de Sanidad (en adelante DGSIES) y Madrid Digital (en adelante MD), validarán el correcto cumplimiento de este formulario e implementarán su solución técnica, siendo responsabilidad del organismo promotor asegurar que los accesos solicitados se ajustan a las necesidades de los acuerdos.

El acceso a los sistemas de información de Atención Primaria se realizará a través de internet mediante la creación de túneles asegurados mediante autenticación y cifrado. En este caso serán **túneles de acceso dinámico** que se establecen directamente desde un ordenador personal (PC) a la red de la CSCM. La configuración del acceso descrita en el manual de usuario se realiza en el PC que deberá tener acceso a internet. Por lo demás, esta configuración no necesita un equipo específico de comunicaciones. Esta opción es necesaria cuando se quiere poder disponer de un acceso en movilidad. (P.ej: accesos desde casa). Los túneles dinámicos se establecen de forma individual por los distintos usuarios que tenga definidos. Siendo necesario dar de alta a los usuarios que se quieran habilitar mediante formulario anexo en este documento. Adicionalmente, estos usuarios deberán firmar el compromiso de confidencialidad.

INSTRUCCIONES PARA CUMPLIMENTAR EL FORMULARIO

1. Todos los campos descritos deben ser rellenados en mayúsculas, es obligatorio cumplimentar los que tienen *.
2. Reglas para los campos con datos personales (no se admitirán usuarios
   - genéricos): Nombres y apellidos completos.
   - Se admitirá el apóstrofe exclusivamente para apellidos como D'ORS, O'DONNELL y nombres propios como HANA'A.
   - No se admitirán signos de puntuación como: punto, coma, dos puntos, acentos, guiones, º, ª, etc., pero si se admitirá la diéresis sobre la U.
   - Se utilizarán exclusivamente los caracteres habituales del alfabeto (norma ISO 3166) incluyendo la Ñ y la Ç.
3. Cumplimentado y firmado el formulario, ha de ser escaneado y enviado por correo electrónico a CESUS cesus@salud.madrid.org. En el caso modificaciones en los servicios accedidos, se adjuntará el formulario de configuración de accesos.
4. Los formularios originales se mantendrán en el organismo que corresponda.
5. Las modificaciones técnicas que se quisieran solicitar sobre el túnel una vez creado se deberán comunicar mediante el envío del formulario original con el que se creó el acceso, junto con los anexos de detalles técnicos que se hayan solicitado anteriormente.
6. Para que exista un correcto control, la baja de los usuarios debe solicitarse y ser autorizado siguiendo el mismo procedimiento de alta de usuarios. Se debe comunicar a CESUS la baja del usuario a través de los medios anteriormente expuestos.
7. Como regla general, tras un periodo de inactividad de seis meses, la cuenta de acceso será desactivada automáticamente. Y en cualquier caso una vez haya finalizado el plazo autorizado.
8. Si se detectara cualquier anomalía en el servicio o ante cualquier duda, el solicitante deberá ponerse en contacto con CESUS a través del teléfono 9137000 00, o bien a través del correo electrónico cesus@salud.madrid.org.

Este formulario incluye *4* anexos:

- **Anexo I. Formulario de alta/baja de acceso a los sistemas de información de Atención Primaria para el grupo GAR_ASISTENCIAL_AP**
- **Anexo II. Formulario solicitud configuración accesos.**
- **Anexo III. Compromiso de confidencialidad.**
- **Anexo IV. Información detallada sobre protección de datos.**

***Definiciones:**
Responsable de la Consejería - gestor del centro de la CSCM responsable de los servicios y bases de datos accedidos o responsable de seguridad.
El solicitante del acceso - responsable de la gestión del acceso en la entidad externa.

ANEXO I. Formulario de alta/baja de acceso a los sistemas de información de Atención Primaria para el grupo GAR_ASISTENCIAL-AP

***Identificador del Acceso:** _____

*Se utilizará en solicitudes sucesivas relativas a este acceso. En la primera solicitud de un acceso deberá requerirse el código a CESUS.

☐ Alta ☐ Baja ☐ Modificación

Información básica sobre Protección de Datos	
Responsable	*Dirección General de Sistemas de Información y Equipamientos Sanitarios de la Consejería de Sanidad de la Comunidad de Madrid*
Finalidad	*Aquella que indica el Título del presente formulario*
Legitimación	*Ejecución contractual (RGPD 6.1.b)*
Destinatarios	*No se cederán datos salvo obligación legal.*
Derechos	*Acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, cuando sean aplicables.*
Información adicional	*Puede consultar la información adicional y detallada sobre Protección de Datos en el Anexo IV.*

ESTE FORMULARIO DEBE SER ARCHIVADO Y CONSERVADO

Datos personales del solicitante (para accesos desde entidades externas de la CSCM)

Nombre (*) _____ Apellido 1 (*) _____ Apellido 2 (*)

NIF/ NIE (*) _____ Correo electrónico (*)

Teléfono de contacto (*) _____ Nombre de la Entidad externa (*)

Cargo del solicitante (*) _____

Datos del contrato que motiva la solicitud

CIF (*)_____ Organismo contratante (*) _____

Título del contrato (*) _____

Datos del responsable de la Consejería de Sanidad que autoriza el acceso

Nombre (*)_____ Apellido 1 (*)_____ Apellido 2 (*) _____

NIF/ NIE (*)_____ Correo electrónico (*) _____

Teléfono de contacto (*) _____

Categoría del responsable de la solicitud (*) _____

Organismo/Dirección/Gerencia (responsable) (*) _____

Unidad o servicio / puesto (*) _____

Datos de los usuarios a dar de alta y/o baja

Nombre	Apellidos	DNI	Función que justifica el acceso

ESTE FORMULARIO DEBE SER ARCHIVADO Y CONSERVADO

Autorización de la

Fecha de la autorización: _____

FIRMA SOLICITANTE:

Firmado:

FIRMA RESPONSABLE DE LA SOLICITUD EN LA CSCM:

Firmado:

ANEXO II. FORMULARIO SOLICITUD CONFIGURACIÓN ACCESOS

Datos responsable Técnico CSCM Nombre y apellidos Dirección email Teléfono	
Fecha	
Dirección/Area	
Centro	
Identificador del Acceso	

Fecha	Alta /Baja	ORIGEN: Red/IP (solo en VPNs estáticas)	Tipo Aplicación (en Accesos dinámicos)	DESTINO - Red/IP	SERVICIO – TCP/UDP	Comentarios	Fecha baja

Tipos de aplicación de Accesos remotos Web/Nativa:
Web → Aplicación de tipología Web en modo portal, es el propio firewall quien realiza la conexión a la aplicación, no requiere de cliente SNX (Connect).
Nativa → Aplicación que requiere de SSL Network Extender, la comunicación se realiza entre el cliente que recibirá una ip y la aplicación (Ejem. Remote Desktop, ssh, telnet, ftp, etc)

Registro de cambios

Incluir en esta tabla los cambios realizados en relación con este acceso, incluyendo los solicitados en este formulario

Fecha	Alta /Baja	ORIGEN: Red/IP (solo en VPNs estáticas)	Tipo Aplicación (en Accesos dinámicos)	DESTINO - Red/IP	SERVICIO – TCP/UDP	Comentarios	Fecha baja

Otras Solicitudes

Breve descripción de la necesidad o anotaciones

Autorización de la solicitud

FIRMA RESPONSABLE Técnico CSCM

Firmado _____

ANEXO III. COMPROMISO DE CONFIDENCIALIDAD

Toda persona que acceda a los sistemas de información de la CSCM, en adelante *el usuario*, deberá leer y aceptar el presente compromiso de confidencialidad:

El *usuario*, en el desempeño de sus funciones, podrá acceder a los datos contenidos en los sistemas de información, incluidos los datos personales especialmente protegidos según la legislación vigente. El *usuario* declara conocer que únicamente se le otorga el acceso a la red a través de este formulario, para **ejercer las funciones que tiene asignadas como trabajador perteneciente a las Unidades de Atención en las Residencias sociosanitarias (UAR) o como personal destinado a atención domiciliaria**, siendo consciente de que este acceso quedará retirado en el momento en el que cese en el cargo descrito. El personal tendrá acceso, a través de VPN a la aplicación AP Madrid, dentro de su horario laboral.

Asimismo, el *usuario* se compromete a:

- Limitar su acceso a los datos y operaciones que sean imprescindibles para el desarrollo del servicio correspondiente, durante el tiempo estrictamente necesario.
- Mantener el más escrupuloso secreto acerca de los datos accedidos, incluso después de finalizada la relación con la CSCM.
- Una vez finalizada la relación, los datos que trate deberán ser destruidos o devueltos a la CSCM.
- Custodiar diligentemente y no compartir su clave de acceso.
- No imprimir, ni extraer datos fuera de los sistemas de información de la CSCM.
- No acceder a datos personales si el acceso no está justificado por el desempeño de las funciones propias de su puesto. Comunicar, a la mayor brevedad, y de conformidad con el procedimiento establecido al efecto, cualquier incidencia que pueda afectar a la seguridad de los datos.
- Solicitar la cancelación de su acceso una vez finalizada la relación con la CSCM, o cuando la confidencialidad de su clave de acceso haya podido verse comprometida.
- El *usuario* declara conocer y se compromete a respetar todas las normas y medidas de seguridad aplicables para el tratamiento de datos de carácter personal, así como la *Política de Seguridad de la Información en el Ámbito de la Administración Electrónica y de los Sistemas de Información de la Consejería de Sanidad de la Comunidad de Madrid, aprobada por la Orden 491/2013, de 27 de junio*.
- Adicionalmente, se han definido una serie de directrices, específicas para el teletrabajo, que deben cumplirse para mantener la seguridad de la información y cumplir con la normativa de protección de datos:
    - Debe tenerse la mayor **diligencia y cuidado** posible con los **dispositivos externos** para evitar daños, averías, pérdidas o sustracciones. No dejarlos sin supervisión a la posible vista de terceros (por ej., vehículo, lugar público, etc.).
    - Evitar el envío de información confidencial o de documentos que contengan datos personales mediante correo electrónico y, si es imprescindible hacerlo, utilizar **exclusivamente el correo corporativo**, no poner datos en el asunto y que la documentación no vaya en el cuerpo del correo, sino en un documento adjunto y con acceso cifrado.
    - Recordamos la obligación de dar cumplimiento al **deber de secreto y confidencialidad** de la información a la que se tenga acceso en el desempeño de sus funciones. Por ello, tanto en lugares públicos como en el entorno doméstico es obligado adoptar las precauciones necesarias para garantizar la confidencialidad de la información que se está gestionando.
    - De igual manera, si habitualmente se genera y trabaja con papel, durante situaciones de movilidad es importante **minimizar o evitar la entrada y salida de documentación** en este soporte y extremar las precauciones para evitar accesos no autorizados por parte de terceros.

- La **información en** soporte **papel**, incluyendo borradores, no se puede desechar sin garantizar que es adecuadamente **destruida**. Si es posible, no arrojar papeles enteros o en trozos en papeleras de hoteles, lugares públicos o en la basura doméstica a los que alguien podría acceder y recuperar información de carácter personal.

- Se debe **evitar exponer la pantalla a miradas de terceros**. Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.

- En la medida de lo posible es aconsejable **prevenir que se puedan escuchar conversaciones por parte de terceros** ajenos utilizando, por ejemplo, auriculares o retirándose a un espacio en el que la persona empleada no esté acompañada.

- **No debe usarse conversores gratuitos** sobre documentos que contengan información confidencial o datos personales (convertidores de PDF a Word, etc.).

- Es recomendable **revisar y eliminar periódicamente la información residual** que pueda quedar almacenadas en el dispositivo, como archivos temporales del navegador o descargas de documentos.

- Debe **activarse** la protección **antivirus** con el fin de evitar posibles infecciones en nuestro equipo de trabajo, o evitarlas en la medida de lo posible.

- **Deben bloquearse las pantallas** del ordenador y los dispositivos móviles, al igual que se hace en el puesto de trabajo habitual, para que no sean accesibles a terceros.

El usuario confirma que entiende y acepta los anteriores requisitos, y se compromete a cumplirlos:

Fecha **DNI**

Firmado _____

ANEXO IV. INFORMACIÓN DETALLADA SOBRE PROTECCIÓN DE DATOS

Información básica sobre Protección de Datos	
Responsable	Responsable del Tratamiento: Dirección General de Sistemas de Información de la Consejería de Sanidad de la Comunidad de Madrid Domicilio: Plaza Carlos Trías Bertrán nº7 (Edif. Sollube) Madrid 28020. Delegado de Protección de Datos: Comité Delegado de Protección de Datos de la Consejería de Sanidad de la Comunidad de Madrid, en Plaza Carlos Trías Bertrán nº7 (Edif. Sollube) Madrid 28020.
Finalidad	Aquella que señala el nombre del formulario del que se remite a esta información.
Legitimación	La base jurídica que legitima el tratamiento es la ejecución de un contrato.
Destinatarios	Sus datos no serán cedidos, salvo en los casos obligados por Ley.
Derechos	Podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, en la medida que sean aplicables, a través de comunicación escrita al domicilio arriba descrito al Responsable del Tratamiento, concretando su solicitud, junto con su DNI o documento equivalente. Le informamos de la posibilidad de presentar una reclamación ante la Agencia Española de Protección de Datos.