Servicio Andaluz de Salud
Consejería de Salud y Consumo

ayudaDIGITAL AL PROFESIONAL SAS

SOLICITUD VPN SEDE CONTRA SEDE
CONEXIÓN AL SISTEMA SANITARIO PÚBLICO DE ANDALUCÍA

A) TIPO DE SOLICITUD

- ○ **AMPLIACIÓN DE VISIBILIDAD** SOBRE UNA VPN SEDE A SEDE EXISTENTE
- ◉ **ALTA** VPN SEDE A SEDE

B) DATOS VPN SEDE A SEDE (ÚNICAMENTE EN CASO DE AMPLIACIÓN)

EMPRESA	
CÓDIGO VPN	
IP VPN (DIR. PRIVADO)	

C) DATOS DE LA CONEXIÓN VPN S2S SOLICITADA (ÚNICAMENTE EN CASO DE ALTA)

ES RESPONSABILIDAD DE LA EMPRESA DISPONER DE LA INFRAESTRUCTURA NECESARIA PARA LA CONFIGURACIÓN DEL TÚNEL IPSEC EN SUS INSTALACIONES.

NÚMERO DE IPS QUE SE USARÁN EN EL EXTREMOS DE LA EMPRESA SOLICITANTE DE MANERA **SIMULTÁNEA**	
IP PÚBLICA DE LA EMPRESA SOLICITANTE, DESDE LA QUE SE ESTABLECERÁ EL TÚNEL IPSEC CON LA JUNTA DE ANDALUCÍA	

D) IDENTIFICACIÓN DE LA EMPRESA Y REPRESENTANTE LEGAL (OBLIGATORIO)

EMPRESA

NOMBRE EMPRESA	
NIF	
DIRECCIÓN	

REPRESENTANTE LEGAL (Datos del representante legal de la empresa o persona con la debida potestad para autorizar la solicitud de acceso a la Red Corporativa de la Junta de Andalucía, asumiendo así las connotaciones legales que este acceso conlleva)

APELLIDOS		NOMBRE		DNI	
TELÉFONO		CORREO-E			

E)IDENTIFICACIÓN DE CONTACTOS EN LA EMPRESA

RESPONSABLE TIC DE LA EMPRESA (OBLIGATORIO)

APELLIDOS		NOMBRE	
TELÉFONO		CORREO-E	

DELEGADO DE PROTECCIÓN DE DATOS (DPD) (OBLIGARIO SI APLICA EN LA EMPRESA)

APELLIDOS		NOMBRE	
TELÉFONO		CORREO-E	

REPONSABLE DE SEGURIDAD TIC (RSEG) (OBLIGATORIO)

APELLIDOS		NOMBRE	
TELÉFONO		CORREO-E	

CONTACTO TÉCNICO CONTACTO PARA LA CONFIGURACIÓN DEL TÚNEL IPSEC. (OBLIGATORIO)

APELLIDOS		NOMBRE	
TELÉFONO		CORREO-E	

F) PROYECTO ASOCIADO POR EL QUE SE SOLICITA EL ACCESO

Se incluirá una breve explicación del proyecto que justifique la necesidad de conexión de la empresa solicitante con la Red Corporativa de la Junta de Andalucía, junto a la relación de centros SAS a los que se solicita el acceso.

BREVE EXPLICACIÓN DEL PROYECTO Y JUSTIFICACIÓN DEL ACCESO (OBLIGATORIO)

CENTROS DEL SAS PARA LOS QUE SOLICITA EL ACCESO (OBLIGATORIO)

G) PROYECTO ASOCIADO POR EL QUE SE SOLICITA EL ACCESO (OBLIGATORIO PARA CADA ACCESO DETALLAR TODA LA INFORMACIÓN)

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

APLICACIÓN, DATOS O RED	
IPS DESTINO	
PUERTOS	

H) FIRMA DEL REPRESENTANTE LEGAL DE LA EMPRESA (OBLIGATORIO)

El Representante legal abajo firmante solicita para su empresa, indicada en el apartado **D**, acceso vía VPN a datos del Servicio Andaluz de Salud según las condiciones especificadas. Asimismo, el Representante Legal **se compromete a notificar a SAS cualquier cambio en la relación profesional o de gestión de proyecto que afecte al servicio solicitado.**

FECHA: FIRMADO:

ANEXO I (OBLIGATORIO)

BUENAS PRÁCTICAS, CLAUSULAS DE CONFIDENCIALIDAD Y CLAUSULAS DE INFORMACIÓN EN LA RECOGIDA DE DATOS PERSONALES PARA EMPRESAS U ORGANISMOS EXTERNOS.

Conste por el presente documento que

D./Dª. ,

con DNI/NIF ,

Representante Legal de la empresa

Al firmar la solicitud y aceptar el uso de acceso remoto, la empresa u Organismo externo que solicita alta en el Servicio VPN se compromete a cumplir los términos y condiciones expuestos a continuación:

1. Observar el cumplimiento de las obligaciones en materia de confidencialidad y protección de datos de carácter personal de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).
2. Observar en el uso de aplicaciones y sistemas del SAS el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía, aprobado por Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública. C
3. **Comunicar a la Subdirección de Tecnologías de la Información y Comunicaciones de cualquier modificación contractual que afecte a sus derechos de acceso, especialmente al finalizar su relación con el Servicio Andaluz de Salud para revocar este acceso.**
4. Guardar la confidencialidad de la información incorporada los sistemas a los que acceda.
5. Hacer uso pertinente y profesional del acceso a las redes de comunicación.
6. Hacer un buen uso del acceso a Internet a través de la red corporativa, extremando las medidas de seguridad en los equipos y aplicaciones.
7. Hacer un uso profesional de las aplicaciones informáticas a las que se accede.
8. El personal con responsabilidades en los sistemas de información no accederá a la misma aprovechando sus privilegios de administración.
9. Asegurarse de el equipo remoto dispone de las medidas de seguridad requeridas conforme a la categoría de los sistemas de información a los que accede (mantener sistema operativo y aplicaciones actualizados, protección de código dañino activa y actualizada, firewall activo, etc).
10. Asegurarse de que su antivirus se mantenga actualizado y realice análisis programados periódicos exhaustivos, incluyendo unidades removibles, incluso aunque no se reinicie el equipo remoto.
11. Aplicar las actualizaciones programadas.
12. Cerrar su conexión cuando ya no sea necesario para evitar su utilización por terceras personas que pudieran tener acceso al equipo remoto.
13. Cerrar las aplicaciones correspondientes a sistemas del Servicio Andaluz de Salud cuando no las esté utilizando (logout).
14. Tener especial cuidado con las unidades de disco compartidas.
15. Prever mecanismos que permitan el reinicio de estas máquinas de forma remota y acceder por canales establecidos a las mismas desde fuera, una vez se reiniciara el equipo. Se recomienda tener un listado de las direcciones IP de los posibles orígenes remotos de las conexiones.
16. Tener activados servicios de monitorización con alertas definidas.
17. En el caso de que almacene información de pacientes o confidencial en su equipo remoto recuerde que debe estar autorizado para ello y que esta información debe almacenarse debidamente cifrada mediante mecanismos debidamente autorizados y certificados.

Por otra parte, en cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD), le informamos que:

- El responsable del tratamiento de sus datos es la Dirección General de Gestión Económica y Servicios del Servicio Andaluz de Salud.
- Estos datos son necesarios para darle de alta y asignarle una VPN y con esta finalidad los trataremos al amparo de lo dispuesto en el artículo 6.1.b) del RGPD, esto es, la ejecución de un contrato.
- Usted puede ejercer sus derechos de acceso, rectificación, supresión, así como otros derechos, según se explica en la información adicional publicada en: https://www.juntadeandalucia.es/servicioandaluzdesalud/proteccionde-datos

FECHA: FIRMADO: