# Solicitud Acceso Red Corporativa

# Servicio Andaluz Salud

# Granada

Versión del documento: **1.06**

Fecha **03 de octubre de 2025**

## TABLA DE ESTADO

| Identificador | Origen | Estado | Versión | Fecha de la revisión |
|---|---|---|---|---|
| SolicitudAccesoRedGR | Interno | Publicado | 1.05 | 12/07/2024 |
| **Autores:** | Nicolás Barajas García, Carmen Mena Gallardo | | | |
| **Clasificación** | Restringido | **GRPD** | n/a | |
| **Administrador** | | | | |
| **Aprobado por** | Antonio Cristóbal Delgado Matas | | **Fecha** | 02/03/2021 |
| **Distribución:** | | | | |
| **Resumen:** | Documento donde se detallan el procedimiento a seguir para crear la documentación de diseño y administración de nuevos entornos se detalla la solicitud de acceso a red por parte de cualquier proveedor externo, de cualquier dispositivo de red. | | | |
| **Palabras clave:** | SOLICITUD ACCESO RED PROVEEDORES EXTERNOS | | | |

## TABLA DE CONTROL DE VERSIONES

| Versión | Fecha | Cambios | Autores |
|---|---|---|---|
| 1.0 | 09/03/2020 | Creación del documento, evolución de antiguo documento de Reserva de IP Granada. | Nicolás Barajas García |
| 1.2 | 15/02/2021 | Se amplia y mejora documento. | Nicolás Barajas García |
| 1.3 | 3/08/2023 | Se amplia configuración microClaudia, DNS’s, NTP e IPv6. Consideraciones USTIC. Se añade Anexo configuración de protocolos. | Carmen Mena Gallardo |
| 1.4 | 05/07/2024 | Se elimina la referencia al antivirus Symantec. | Carmen Mena Gallardo, José Garrido, Ana Chamocho. |
| 1.5 | 21/08/2024 | Se habilita los campos que no son rellenables. | José Garrido |
| 1.6 | 25/09/2025 | Se amplían campos: marca, modelo, denominación GMD, forma de adquisición y garantía. | Ana Chamocho Ayuso |

## ÍNDICE

1 ALCANCE.....6

2 CONSIDERACIONES UNIDAD SEGURIDAD TIC SAS.....7

3 CONDICIONES EXIGIBLES Y REQUERIDAS.....9

3.1 REQUISITOS CONEXIÓN DE EQUIPOS.....9

4 DATOS SOLICITUD.....10

4.1 DATOS DEL SOLICITANTE.....10

4.2 DATOS UNIDAD/SERVICIO HOSPITAL.....10

4.3 NUEVO DISPOSITIVO EN RED SAS.....10

4.4 MODIFICACIÓN DISPOSITIVO EXISTENTE EN RED SAS.....10

5 AUTORIZACIÓN RESPONSABLE TIC.....11

6 CONSIDERACIONES TIC GRANADA.....12

7 NORMA EXIGENTE.....13

# 1 ALCANCE

El presente documento está destinado a solicitar acceso de cualquier tipo de dispositivo a la subred de los centros del SSPA en la provincia de Granada en el marco de la Red Corporativa de la Junta de Andalucía (RCJA) y del Servicio Andaluz de Salud. Entendiéndose por dispositivo un PC, impresora, dispositivo IoT, equipamiento electro-médico, etc. En definitiva, cualquier dispositivo de red diferente a un servidor alojado en CPD.

En función de si es necesario conectar un nuevo dispositivo (apartado Nuevo dispositivo) o sustituir uno existente (apartado Modificación dispositivo), se deberá cumplimentar un apartado u otro teniendo en cuenta que todos los campos son obligatorios.

# 2 CONSIDERACIONES UNIDAD SEGURIDAD TIC SAS

En el caso del equipamiento electro-médico y de conformidad con el Reglamento (UE) 2017/745 sobre productos sanitarios (MDR), el fabricante deberá incluir en su documentación técnica los requisitos generales de seguridad y funcionamiento de estos.

En el caso de un programa informático (software) considerado como producto sanitario o componente de este, el fabricante deberá aportar la guía de configuración segura del producto, es decir, los requisitos mínimos relativos al soporte físico, las características de las redes informáticas y las medidas de seguridad informática necesarios para ejecutar el programa de la forma prevista. Si las medidas de seguridad para el funcionamiento del producto aportadas por el fabricante no son compatibles con las medidas requeridas para la conexión de equipos y servicios en el SAS, en la Guía 012 de Requisitos mínimos de ciberseguridad para el equipamiento electro-médico, la USTIC plantea una serie de medidas de seguridad a aplicar con el fin de minimizar los riesgos, sin dejar atrás el cumplimiento de los requerimientos legales en cuanto a la protección de la información y salud de los pacientes.

# 3 CONDICIONES EXIGIBLES Y REQUERIDAS

## REQUISITOS CONEXIÓN DE EQUIPOS

Con carácter general, la conexión de equipos y servicios de terceros requiere:

1. **Mantener el inventario de equipamiento, monitorización de los equipos** a fin de aplicar las actualizaciones y parches de seguridad proporcionadas por cada fabricante, tan pronto estén disponibles.

**Control de Inventario (agente OCS), agente Altiris o de forma excepcional bajo la responsabilidad del proveedor.**

**Auditoría del equipo** una vez conectado a la red del hospital se comunicará al proveedor las vulnerabilidades encontradas (Tarea Jira para analizar el equipo, antivirus…).

Será responsabilidad del proveedor proporcionar e instalar las actualizaciones del sistema operativo. Así como la aplicación de cualquier medida de seguridad adicional necesaria para garantizar la seguridad.

2. **Instalación de soluciones de seguridad.**

En caso de que el dispositivo pueda llevar instalado un software de seguridad se instalarán los siguientes productos proporcionados por el área TIC:

**El proveedor deberá mantenerlo actualizado durante toda la vida útil del dispositivo**

1. La **protección Microclaudia** contra malware de tipo ransomware de sistemas Windows del CCNCERT.

Más información: Enlace Microclaudia

2. **EndPoint Detection Response (EDR)** Corporativo: **Crowdstrike**.

Los problemas al instalar estas soluciones se deben analizar por parte del área TIC del hospital y el equipo técnico de la USTIC.

En caso de que el dispositivo NO pueda llevar instalado un software de seguridad , y/o no es posible la aplicación de parches críticos y de seguridad, se deben implementar medidas compensatorias para mitigar ese riesgo (ejemplo implementar un FW para aislar el equipo, parcheo virtual, etc.). Dichas medidas deben ser comunicadas y evaluadas por el equipo TIC (Sistemas e Infraestructuras) para su autorización en función de la normativa vigente por la Subdirección TIC Provincial.

**En caso de concederse el acceso al equipo sin soluciones de seguridad se exime a STIC Granada de cualquier responsabilidad ante posibles fallos o mal funcionamiento del dispositivo.**

3. **Aplicar políticas de mínimo privilegio**. Bastionado (hardening) de todos aquellos protocolos de red y servicios no necesarios en el sistema y/o limitar el uso de los mismos. Uso de listas blancas.

4. **Segregación de red.** Los equipos afectados se configurarán aplicando segmentación de red, control de acceso a la red o detrás de firewalls con acceso restringido que solo permita la comunicación con equipos confiables en otras redes. Se monitorizará el tráfico de red que llega a los equipos afectados en busca de actividad sospechosa con el Sistema de Alerta Temprana del CCN-CERT y se comunicará al proveedor caso de producirse una alerta para que realize las acciones recomendadas.

5. **Integración en directorio activo corporativo DMSAS**, o en su caso, medidas compensatorias como gestión de usuarios y contraseñas del sistema acordes a la normativa de control de accesos del SAS**.**

**6.** Se limitará el acceso físico solo al personal autorizado.

**STIC Granada tendrá la plena potestad para aplicar las medidas necesarias contra dicho dispositivo en caso de que suponga un riesgo para la red o resto de equipamiento. Avisando, si es posible, al servicio afectado indicado en el apartado 4.**

# 4 DATOS SOLICITUD

***Todos los campos son obligatorios.***

## DATOS DEL SOLICITANTE

| | |
| --- | --- |
| NOMBRE DEL SOLICITANTE | |
| CARGO | |
| EMAIL | |
| TELÉFONO CONTACTO | |
| NOMBRE EMPRESA | |
| • EMAIL SOPORTE | |
| • TELÉFONO SOPORTE | |

## DATOS UNIDAD/SERVICIO HOSPITAL

| RESPONSABLE: Servicio Hospitalario que autoriza la instalación del dispositivo. | |
| --- | --- |
| Nombre y apellidos | |
| SERVICIO | |
| EMAIL | |
| TELÉFONO CONTACTO | |
| CENTRO HOSPITALARIO | |

## NUEVO DISPOSITIVO EN RED SAS

| | | |
|---|---|---|
| **NOMBRE** | | |
| **MARCA** | | |
| **MODELO** | | |
| **N.º SERIE** | **DIRECCIÓN MAC** | **SISTEMA OPERATIVO** |
| | | |
| **CÓDIGO MANSIS** | **CÓDIGO EQUIPO (GMND)** | **FECHA FIN DE GARANTÍA** |
| | | |
| **FORMA DE ADQUISICIÓN** (Comprado, Cedido, Préstamo, Donado, Demo...) | | |

| | | | |
|---|---|---|---|
| **CENTRO** | | **SERVICIO** | **PLANTA** |
| | | | |
| **EXISTE PUNTO DE RED** | ☐ SI ☐ NO | **IDENTIFICACIÓN DE ROSETA** | |
| **MICROCLAUDIA** | ☐ SI ☐ NO | **ANTIVIRUS ALTERNATIVO** | |
| **EDR CORPORATIVO** | ☐ SI ☐ NO | **PARCHES CRÍTICOS/SEGURIDAD** | ☐ SI ☐ NO |

| |
|---|
| **MEDIDAS COMPENSATORIAS SI NO INSTALA SW DE SEGURIDAD NI PARCHES** |
| |

| | |
|---|---|
| **NECESIDAD IP RESERVADA** | ☐ SI ☐ NO |

| |
|---|
| **JUSTIFICACIÓN NECESIDAD IP RESERVADA POR DHCP** |
| |
| **FUNCIONALIDAD/DESCRIPCIÓN DISPOSITIVO Y OTRAS OBSERVACIONES RELEVANTES** |
| |
| **PROTOCOLOS Y PUERTOS NECESARIOS PARA FUNCIONAMIENTO** |
| |

## MODIFICACIÓN DISPOSITIVO EXISTENTE EN RED SAS

| | | |
|---|---|---|
| **NOMBRE** | | |
| **MARCA** | | |
| **MODELO** | | |
| **N.º SERIE** | **DIRECCIÓN MAC ANTÍGUA** | **DIRECCIÓN MAC NUEVA** |
| | | |
| **CÓDIGO MANSIS** | **CÓDIGO EQUIPO (GMND)** | **FECHA FIN DE GARANTÍA** |
| | | |
| **FORMA DE ADQUISICIÓN** (Comprado, Cedido, Préstamo, Donado, Demo...) | | |

| | | | |
|---|---|---|---|
| **CENTRO** | | **SERVICIO** | **PLANTA** |
| | | | |
| **EXISTE PUNTO DE RED** | ☐ SI ☐ NO | **IDENTIFICACIÓN DE ROSETA** | |
| **MICROCLAUDIA** | ☐ SI ☐ NO | **ANTIVIRUS ALTERNATIVO** | |
| **EDR CORPORATIVO** | ☐ SI ☐ NO | **PARCHES CRÍTICOS/SEGURIDAD** | ☐ SI ☐ NO |
| **MEDIDAS COMPENSATORIAS SI NO INSTALA SW DE SEGURIDAD NI PARCHES** | | | |
| | | | |
| **NECESIDAD IP RESERVADA** | ☐ SI ☐ NO | IP RESERVADA A MANTENER | |
| **JUSTIFICACIÓN NECESIDAD IP RESERVADA POR DHCP** | | | |
| | | | |
| **FUNCIONALIDAD/DESCRIPCIÓN DISPOSITIVO Y OTRAS OBSERVACIONES RELEVANTES** | | | |
| | | | |
| **PROTOCOLOS Y PUERTOS NECESARIOS PARA FUNCIONAMIENTO** | | | |
| | | | |

# 5 AUTORIZACIÓN RESPONSABLE TIC

Se requiere al menos una autorización de algún responsable TIC (Gestión de Proyectos, SPU, Referente del proyecto, Referente del centro) para la concesión de acceso a red del dispositivo en caso de incumplimiento de las medidas básicas definidas en este documento.

| AUTORIZACIONES TIC GRANADA | |
| --- | --- |
| NOMBRE DEL RESPONSABLE | |
| PROYECTO CONFLUENCE | |
| FIRMA | |
| | |
| NOMBRE DEL RESPONSABLE | |
| FIRMA | |
| | |

# 6 CONSIDERACIONES TIC GRANADA

# 7 NORMA VIGENTE

1. Esquema Nacional de Seguridad (ENS).
2. Normativa de uso de los recursos y de los sistemas de información de la Consejería. Comité de Seguridad TIC de la Consejería.
3. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD y RGDD).
4. En el caso del equipamiento electro-médico, conformidad con el Reglamento (UE) 2017/745 sobre productos sanitarios (MDR).