Junta de Andalucía

Consejería de Sanidad, Presidencia y Emergencias

GRANADA
ES SALUD PÚBLICA

Anexo XII

Anexo TIC. Sede definitiva AESAP en Centro Doctor Olóriz

Candidatura de Granada como sede para la Agencia Estatal de Salud Pública (AESAP)

INFRAESTRUCTURA TECNOLÓGICA Y CAPACIDADES DIGITALES COMO VENTAJA COMPETITIVA DEL CENTRO

La candidatura de nuestro centro para albergar la futura **Agencia Estatal de Salud Pública** se sustenta, entre otros pilares, en una **infraestructura tecnológica de alto nivel** que garantiza una operativa robusta, segura, interoperable y preparada para los retos presentes y futuros de la salud pública en el siglo XXI.

Contamos con un conocimiento y experiencia tecnológica evolucionada, una infraestructura centralizada en un Centro de Proceso de Datos (CPD) provincial, cuya infraestructura está desplegada de forma modular y escalable, con capacidades que permiten soportar tanto la actividad asistencial de alta complejidad como entornos de investigación, análisis de datos de salud pública locales, entornos de formación o la posibilidad de desarrollo de nuevas necesidades.

- Capacidades clave:

- **Centro de datos de alta disponibilidad**, con redundancia, respaldo eléctrico y medidas avanzadas de protección física y lógica.
- **Conectividad segura con la Red Corporativa de la Junta de Andalucía (RCJA)**
- **Entornos virtualizados y segmentados** para garantizar la integridad y confidencialidad de los datos.
- Plataforma de servicios preparada para albergar sistemas **basados en análisis de datos, sistemas de información asistenciales, sistemas de información de gestión, sistemas de información económicos, trazabilidad de procesos críticos y toma de decisiones en tiempo real.**

- Ventaja diferencial

Nuestra experiencia en despliegue y evolución de sistemas tecnológicos complejos en el entorno sanitario nos posiciona como un centro idóneo para asumir el reto de alojar y apoyar técnicamente a la futura Agencia.

Además, **nuestra integración con los sistemas provinciales y regionales** facilita la futura interoperabilidad con múltiples actores del sistema de salud, incluyendo centros de investigación, universidades, autoridades sanitarias, residencias, instituciones penitenciarias, empresas tecnológicas, etc.

- Preparados para la salud pública del futuro

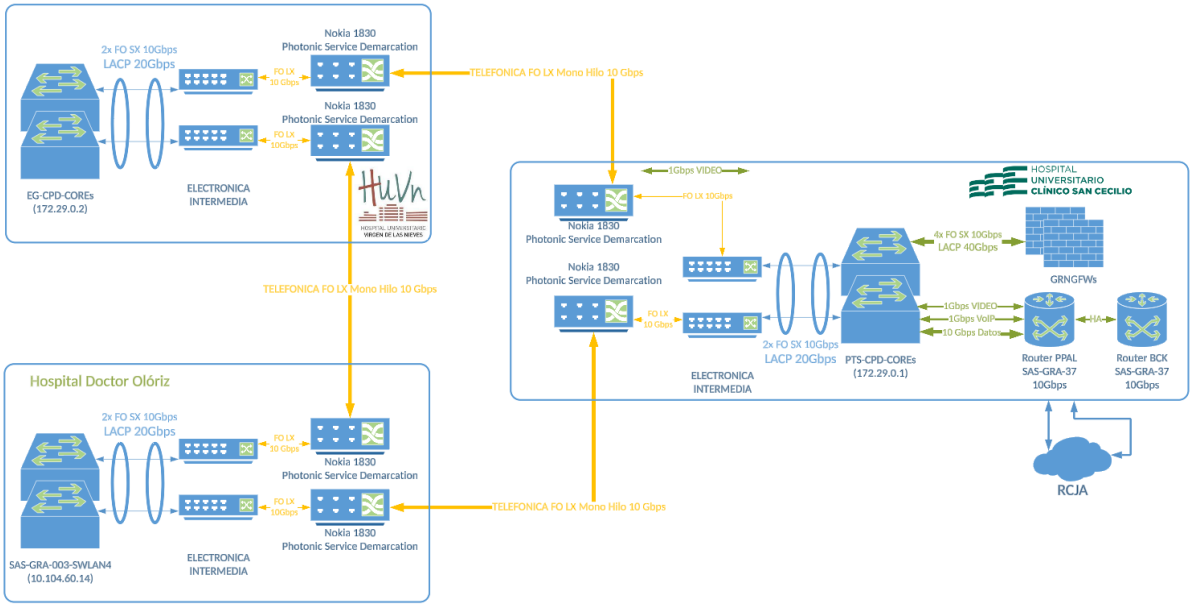
Actualmente se está diseñando la evolución tecnológica de nuestro CPD para ampliar sus capacidades y estar preparados para evolucionar de forma ágil y sostenible en ámbitos como:

- Integración de datos multifuente (clínicos, ambientales, genómicos, sociales).
- Ciberseguridad en contextos de salud pública.
- Ampliación de la capacidad para proyectos de investigación de gran envergadura
- Dotación de la infraestructura necesaria para incorporar la inteligencia artificial en nuestros sistemas

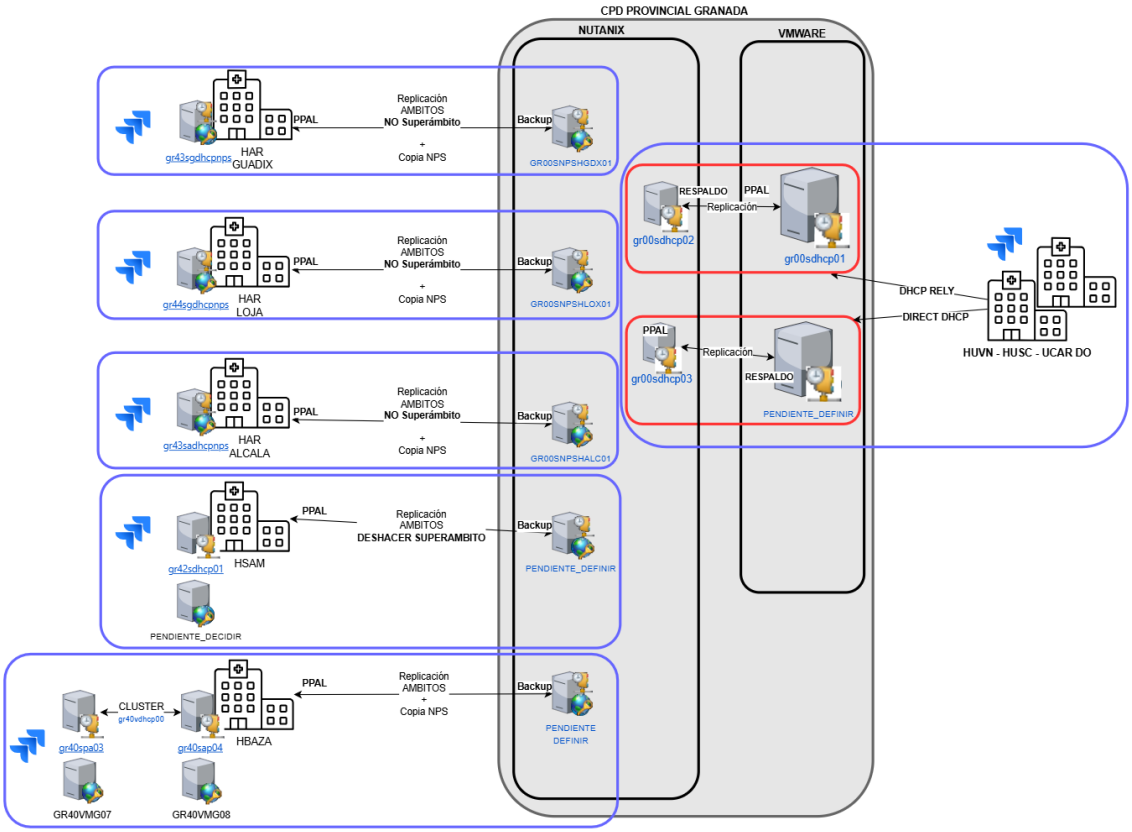
Por todo ello, presentamos nuestra infraestructura como **garantía de viabilidad operativa y seguridad tecnológica** para la instalación y desarrollo de la Agencia Estatal de Salud Pública.

CONFIGURACIÓN RED GRANADA

Actualmente a nivel de comunicaciones de red, los hospitales cuentan con un anillo de comunicaciones implantado entre los edificios principales del Hospital Universitario Virgen de las Nieves, Hospital Universitario Clínico San Cecilio y Hospital Doctor Olóriz, de manera que se pueda dar servicio de comunicaciones ante cualquier eventualidad. Para ello se ha diseñado un anillo de comunicaciones que invierte su flujo de tráfico de red si existiese una rotura de fibra. Además, se ha ampliado el caudal de salida a 10 Gbps hacia la Red Corporativa de la Junta de Andalucía (RCJA) desde el CPD provincial y por tanto la salida a la red externa tanto en la línea principal como la línea de respaldo o backup ya es de 10 Gbps.



Además, el resto de hospitales y centros que engloba a nivel de infraestructura de red la provincia de Granada como el HAR de Guadix, el HAR de Alcalá la Real, el HAR de Loja, el Hospital de Motril, el Hospital de Baza, también está gestionada por nuestro equipo TIC de forma homogénea:



SEGURIDAD PERIMETRAL DE LA RED, UNA PRIORIDAD INELUDIBLE

En un ecosistema hospitalario digitalizado, la **información es el activo más valioso**. Con miles de profesionales y dispositivos conectados a diario, proteger la red interna no es una opción, es una obligación crítica para garantizar la continuidad asistencial, la privacidad de los pacientes y el funcionamiento de los sistemas sanitarios.

La seguridad no se limita a gestionar contraseñas o accesos. Implica el diseño e implantación de **estrategias integrales de protección,** tanto en redes cableadas como inalámbricas, capaces de **prevenir accesos indebidos, segmentar el tráfico interno y auditar en tiempo real el uso de recursos clave.**

Desde el dominio corporativo DMSAS, se está abordando una transformación que permite controlar quién, cómo y desde dónde accede a los servicios digitales del hospital.

Se trata de dotar a los hospitales de una red interna robusta, segmentada y segura, preparada para albergar sistemas críticos, dispositivos médicos conectados. Se trata de prevenir tanto ataques externos mediante mecanismos como firewall, *como para prevenir los usos indebidos de la red interna propia y tener dicha red controlada y auditada a nivel de accesos, permitiendo/denegando aquel tráfico que se desee y segmentando la red en función de las necesidades.*

Aunque los ataques externos suelen acaparar la atención, las amenazas que se originan dentro de la red interna son, en muchos casos, más complejas de detectar y potencialmente más dañinas. Un actor malintencionado con acceso físico o lógico a nuestra red —por ejemplo, mediante la conexión de un portátil no autorizado— puede utilizar el ancho de banda y los recursos internos para lanzar ataques o comprometer servicios críticos.

Una red sin segmentación, con miles de dispositivos conectados y sin medidas de protección activas, se convierte en un entorno extremadamente vulnerable. No hablamos solo de ataques deliberados con fines ilícitos (como sabotajes o accesos a datos confidenciales), sino también de errores o malas prácticas por parte de usuarios no expertos que pueden tener consecuencias graves.

Prevenir estas situaciones requiere la implantación de mecanismos de seguridad en todos los niveles, tanto en redes cableadas como inalámbricas. Es imprescindible poder auditar en tiempo real quién se conecta a la red, desde qué punto, con qué dispositivos y bajo qué credenciales, permitiendo aplicar políticas de acceso adecuadas y garantizando la integridad del ecosistema digital sanitario.

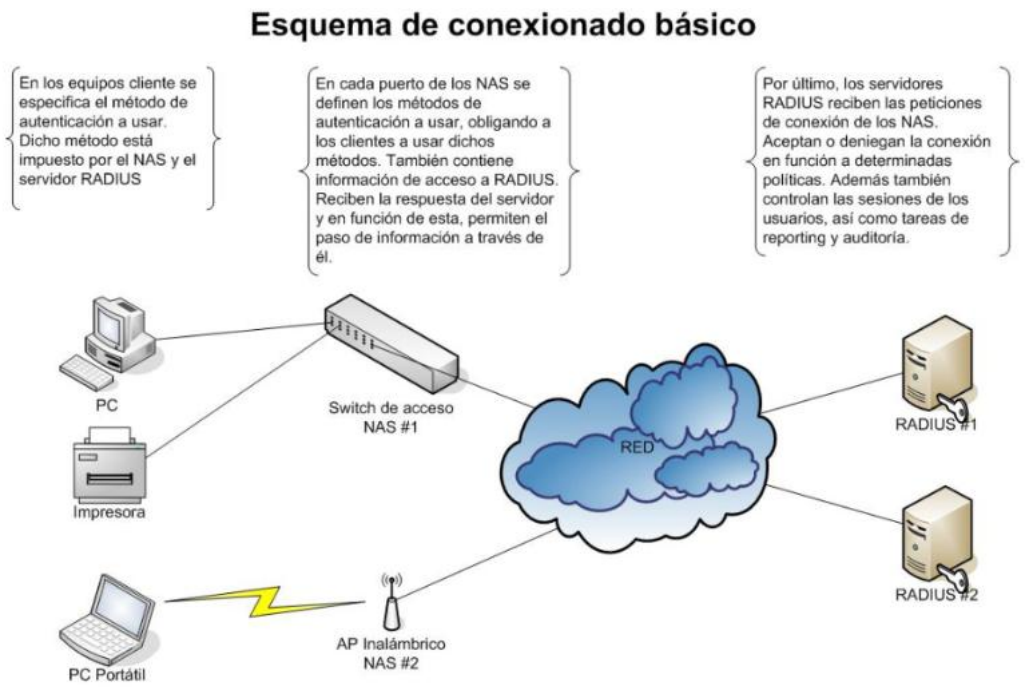
Por ello hay que pretenden cubrir varios escenarios:

1. Accesos no autorizados.
2. Daño intencionado y no intencionado.
3. Uso indebido de información.

Para ello se implantan distintas herramientas como:

- Un sistema de control de acceso a redes (NAC) que proporciona a una entidad un primer nivel de seguridad, cuyas herramientas nos permiten de manera selectiva que usuarios, dispositivos y aplicaciones autorizados obtengan acceso a recursos en red.

- Un servicio RADIUS, que es un protocolo de control de acceso que verifica y autentica usuarios en una sesión de red. Es parte fundamental de un sistema NAC. Además de dar acceso a la red, también se usa para controlar toda la sesión hasta que ésta finalice.



- Sondas de detección temprana de alertas. La implantación de las Sondas SAT ICS (Supervisión de Arquitecturas Tecnológicas en Infraestructuras Críticas de Salud) del CCN-CERT se alinea directamente con la estrategia nacional y hospitalaria de ciberseguridad al:

- Reforzar la vigilancia y defensa de infraestructuras críticas hospitalarias, en línea con las directrices del Esquema Nacional de Seguridad (ENS), la Estrategia Nacional de Ciberseguridad y la protección del sector salud como infraestructura crítica.
- Mejorar la capacidad de detección temprana de ciber amenazas, especialmente en sistemas OT (tecnología operativa), SCADA, dispositivos médicos conectados y redes industriales hospitalarias.
- Facilitar la integración con el Sistema de Alerta Temprana del CCN-CERT, contribuyendo a la inteligencia colectiva y a una respuesta coordinada a incidentes a nivel nacional.
- Dar cumplimiento al Plan de Acción del ENS y a los planes sectoriales de ciberseguridad promovidos por el Ministerio de Sanidad y el INCIBE.

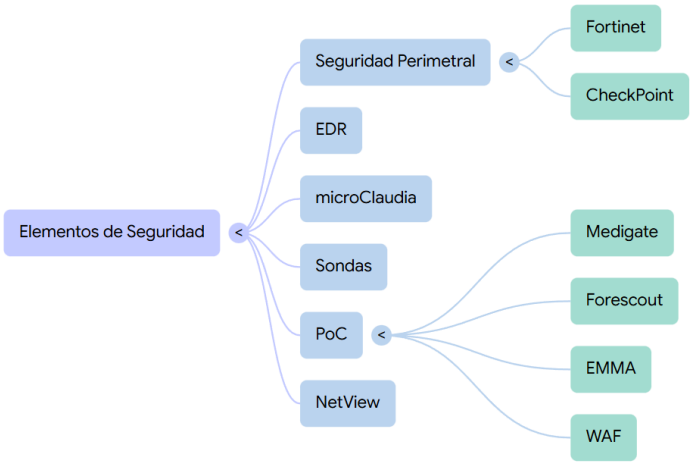
Por qué hacemos esto:

- Las redes OT e ICS del hospital **no están suficientemente monitorizadas** frente a amenazas avanzadas o persistentes.
- **Dispositivos médicos, sistemas de climatización, quirófanos inteligentes, etc.,** están conectados a la red y **podrían ser vulnerables a ataques dirigidos**.
- La organización **carece de visibilidad sobre comportamientos anómalos** en tráfico industrial o interacciones en sistemas no convencionales (no-IT).

Impacto de este problema:

- Potencial **interrupción de servicios clínicos o quirúrgicos críticos** ante un ciberataque.
- **Riesgo elevado para la seguridad física y la salud de los pacientes**.
- **Dificultad para responder o mitigar incidentes** y en tiempo real del tráfico OT.
- Compromiso de **sistemas esenciales como climatización UCI, quirófanos, generadores, etc.** con consecuencias graves.

El siguiente esquema detalla los diversos **componentes de protección** que integran una infraestructura de ciberseguridad organizada. La estructura jerárquica clasifica herramientas esenciales como la **seguridad perimetral**, donde se destacan soluciones de marcas reconocidas como Fortinet y CheckPoint. Otros pilares fundamentales del ecosistema incluyen sistemas de **detección y respuesta (EDR),** así como mecanismos especializados denominados microClaudia y sondas. El diagrama también ilustra una sección de **pruebas de concepto (PoC)** que abarca plataformas de visibilidad y gestión de activos como Medigate y Forescout. Finalmente, se integran funciones de **análisis de red y cortafuegos** de aplicaciones web para garantizar una defensa integral. Esta representación visual facilita la comprensión de cómo se distribuyen las **tecnologías de defensa** para salvaguardar el entorno digital:



GESTIÓN UNIFICADA DE GESTIÓN DE EQUIPAMIENTO EN DIRECTORIO ACTIVO, NETCONTROL

El trabajo realizado del desarrollo de la herramienta NETCONTROL desde Granada como plataforma de gestión del equipamiento en directorio activo DMSAS basado en tecnologías nativas de Microsoft, ha supuesto un avance significativo en la gestión de dispositivos dentro de la red segmentada. La aplicación ha evolucionado hacia un modelo más seguro, eficiente y usable, lo que impacta positivamente en la operatividad del entorno sanitario. Se recomienda continuar con la optimización de procesos y seguridad para garantizar una infraestructura tecnológica robusta y confiable.

Su evolución ha incorporado las siguientes mejoras:

Gestión de Equipos y Colisiones

- Ajustes en la descripción de colisiones en Controller y Model de PCsGestion.
- Implementación de la visualización de PCs Activos y correcciones de errores.
- Mejora en la visualización de número de equipos a borrar en procesos masivos.
- Agregado de logs detallados y barra de progreso en procesos de limpieza.

Integración y Seguridad

- Integración de NetControlVisorVNC con mejoras en la descarga y ejecución en primer plano.
- Mejora en la detección del protocolo VNC para la instalación automatizada.
- Implementación de seguridad en el acceso a los menús de dispositivos y redes.
- Inclusión de un instalador firmado digitalmente para mayor confianza y seguridad.

Optimización de Procesos

- Implementación de Movimiento de Red por Dispositivos y Terminales, con validaciones de MacAddress.
- Mejora en los métodos de cálculo del PC y portátiles siguientes.
- Optimización de la eficiencia en los procesos de asignación y regularización de terminales.
- Mejora en la exportación de datos en PDF y ajustes dinámicos en HTML.

Interfaz y Usabilidad

- Unificación de iconos en las diferentes vistas de la aplicación.
- Mejoras en la barra de menús y visualización de roles de usuario.

- Incorporación de seguridad en accesos y restricciones para usuarios no administrativos.

NUESTRAS REDES VLAN PARA EL EQUIPAMIENTO CONECTADO A RED

Con el objetivo de optimizar la gestión de todo el equipamiento conectado a nuestra red, hemos estructurado redes locales segmentadas por tipología de dispositivo. Esto nos permite agrupar los equipos de forma coherente y mantener su funcionamiento de manera independiente y controlada, distinguiendo entre Equipamiento industrial, Equipamiento IoT y Equipamiento IoMT.

Así tenemos VLANs diferenciadas para Equipamiento de alertas **MYSIRIUS,** Dispositivos electromédicos, Dispositivos de Radiodiagnóstico, Dispositivos de Laboratorio, Dispositivos de Oftalmolgía, Dispositivos de Telemetría, Dispositivos trazabilidad oncológica, Dispositivos quirúrgicos, Impresoras y dispositivos de reprografía como VLANs relevantes que tenemos en nuestros centros.

La segmentación del equipamiento por VLANs no sólo mejora el control y la trazabilidad de los dispositivos conectados, sino que refuerza la seguridad, facilita el diagnóstico de incidencias y permite aplicar políticas de red diferenciadas según el tipo de equipo. En un entorno hospitalario complejo, donde conviven sistemas clínicos, dispositivos biomédicos y servicios administrativos, disponer de una arquitectura en VLANs es clave para garantizar un rendimiento fiable, minimizar riesgos operativos y asegurar la continuidad asistencial.

PLATAFORMA DE AUTOMATIZACIÓN DE RED, NETBRAIN

Nuestro CPD cuenta con **una avanzada plataforma de automatización de red** diseñada para transformar las operaciones tradicionales de gestión de infraestructuras (NetOps). Esta solución permite **automatizar flujos de trabajo críticos sin necesidad de programación**, lo que **aumenta significativamente la escalabilidad operativa y reduce tanto los costes como los riesgos asociados a la gestión manual.**

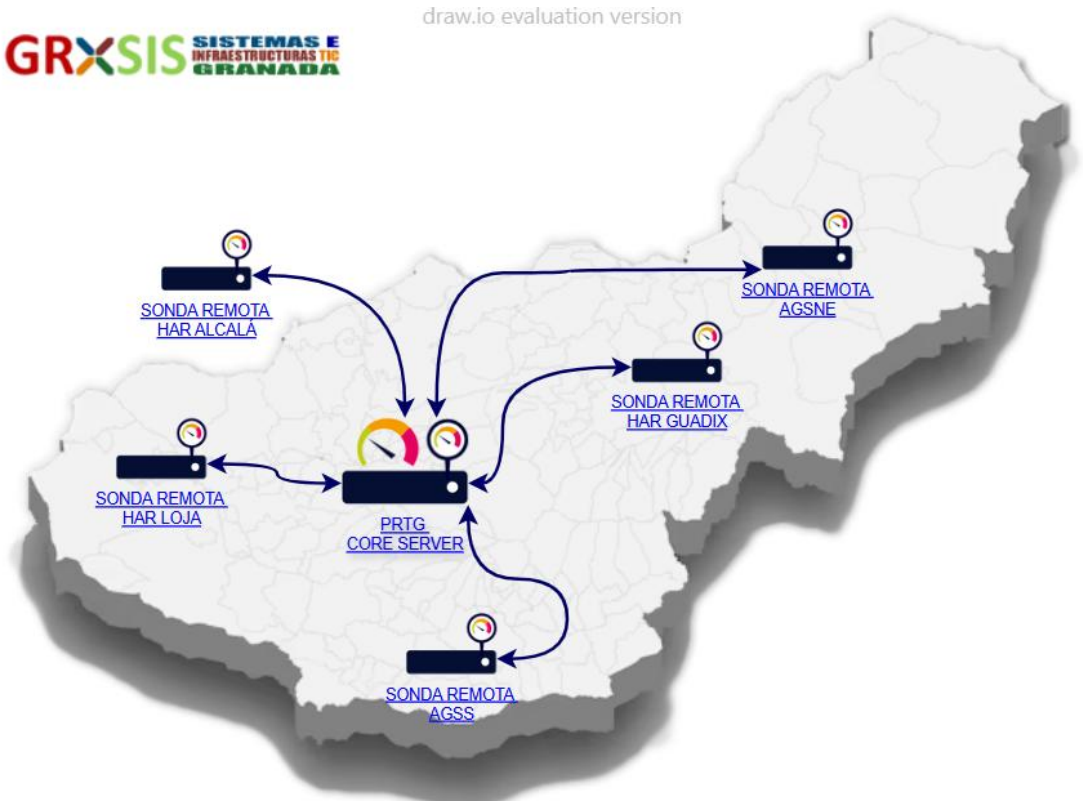
Gracias a esta plataforma, las tareas de configuración, supervisión, diagnóstico y respuesta ante incidencias pueden ejecutarse de forma orquestada, estandarizada y segura, **liberando recursos técnicos para actividades de mayor valor añadido.**

Esta transformación hacia **una red autogestionada y adaptativa** es clave para soportar la creciente complejidad de los entornos hospitalarios actuales, donde la disponibilidad continua, la seguridad y la capacidad de adaptación rápida son esenciales. La **automatización sin código** facilita además que los equipos puedan implementar cambios o nuevas políticas de forma ágil, sin depender de desarrollos específicos, acelerando así la innovación tecnológica dentro del sistema sanitario.

PLATAFORMA DE GESTIÓN DE INCIDENCIAS, PRTG

Se ha implantado un sistema que permite medir el estado de cada infraestructura a través de una única consola, permitiendo un análisis avanzado y centralizado de logs para generación de eventos y alertas. Además de la información que aporta para la gestión, el mantenimiento y la monitorización de los sistemas e infraestructuras permite una gestión de **avisos** de manera que puedan alertar de forma proactiva. Estas herramientas están d**isponibles vía WEB, cliente pesado y APP Móvil**.

Dicho conjunto de herramientas nos permite tener una visión global y de extremo a extremo del estado de los sistemas e infraestructura de forma global, siendo PRTG la plataforma de monitorización única y homogénea para toda la provincia de Granada:



ANDALUCÍACERT

La arquitectura TIC prevista para la sede definitiva de la AESAP se apoya, además, en el modelo corporativo de ciberseguridad de la Junta de Andalucía, articulado a través de AndalucíaCERT, garantizando un marco estable y homogéneo de protección de los sistemas de información

AndalucíaCERT actúa como el Equipo de Respuesta ante Incidentes de Seguridad Informática de la Junta de Andalucía y constituye un elemento estructural del modelo de gobernanza de la ciberseguridad en el ámbito autonómico. Su integración en la arquitectura TIC de la sede definitiva de la AESAP proporciona un marco consolidado de protección, prevención y respuesta ante incidentes de seguridad que puedan afectar a los sistemas de información y comunicaciones de la Agencia.

La adscripción de la infraestructura de red y comunicaciones a este modelo permite disponer de capacidades avanzadas y permanentes de gestión de la ciberseguridad, incluyendo la supervisión continua de eventos de seguridad, la coordinación de respuestas ante incidentes, la gestión de vulnerabilidades y la aplicación de medidas correctivas y preventivas de forma centralizada. Todo ello contribuye a garantizar elevados niveles de disponibilidad, integridad y confidencialidad de la información, en coherencia con los requisitos del Esquema Nacional de Seguridad y con las exigencias propias de una agencia estatal de carácter estratégico.

Asimismo, AndalucíaCERT opera en coordinación con redes nacionales e internacionales de equipos de respuesta a incidentes, facilitando el intercambio de información sobre amenazas, indicadores de compromiso y buenas prácticas en ciberseguridad. Esta cooperación refuerza la capacidad de anticipación frente a riesgos emergentes

y proporciona a la sede definitiva de la AESAP un entorno digital resiliente, preparado para soportar de forma sostenida las funciones críticas de vigilancia, análisis, intercambio de información sensible y apoyo a la toma de decisiones en salud pública.

MADUREZ EN CIBERSEGURIDAD

La arquitectura de seguridad TIC que da soporte a la sede definitiva de la AESAP se sustenta en un modelo organizativo y operativo altamente consolidado, alineado con la Política de Seguridad TIC del Servicio Andaluz de Salud y con la estructura corporativa de seguridad de la Junta de Andalucía. Este modelo integra de forma coherente la seguridad física y lógica, mediante una organización claramente definida de roles, responsabilidades y órganos de gobierno, que incluye comités de seguridad a nivel central y de institución, responsables de seguridad TIC y unidades especializadas con funciones diferenciadas, en plena coherencia con los principios del Esquema Nacional de Seguridad.

En este contexto, la Unidad de Seguridad TIC del Servicio Andaluz de Salud (USTIC) desempeña un papel clave en la implantación, operación y mejora continua de la seguridad, proporcionando capacidades avanzadas de monitorización, detección, respuesta a incidentes, análisis de riesgos, auditoría, formación y concienciación. Esta estructura permite una gestión sistemática y profesionalizada de la ciberseguridad, basada en procesos maduros, métricas de seguridad y mecanismos de mejora continua, plenamente alineados con las exigencias regulatorias actuales y futuras.

La coordinación de este modelo con AndalucíaCERT, como CSIRT de referencia para los organismos de la Junta de Andalucía, garantiza la integración de la sede definitiva de la AESAP en un ecosistema de respuesta a incidentes consolidado, con capacidad de cooperación a nivel nacional e internacional. Un indicador objetivo de esta madurez es la elevada capacidad de detección y notificación de incidentes de seguridad demostrada por el Servicio Andaluz de Salud en los mecanismos nacionales de reporte, situándose de forma consistente entre los organismos públicos con mayor volumen de incidentes gestionados y comunicados. Este hecho no refleja una mayor exposición al riesgo, sino un alto grado de visibilidad, control y cumplimiento de las obligaciones de notificación, aspecto clave en el marco del Esquema Nacional de Seguridad y de la Directiva NIS2.

Este nivel de madurez organizativa y operativa en ciberseguridad proporciona a la sede definitiva de la AESAP un entorno digital robusto, resiliente y preparado para soportar de forma sostenida servicios críticos, tratamiento de información sensible y funciones estratégicas de vigilancia y análisis en salud pública, reduciendo riesgos operativos y reforzando la confianza institucional desde una perspectiva de largo plazo.