PLIEGO DE CONDICIONES TÉCNICAS QUE HABRÁ DE REGIR LA LICITACIÓN, MEDIANTE PROCEDIMIENTO ABIERTO, PARA CONTRATACIÓN DE LOS SERVICIOS DE SOLUCIONES DE SEGURIDAD PERIMETRAL, SWITCHES DE ACCESO, GESTIÓN CENTRALIZADA, ANALÍTICA DE SEGURIDAD Y CONTROL DE ACCESO A RED vinculado a la actuación A21 del proyecto TRADIGUSA susceptible de ser financiado CON FONDOS PROCEDENTES DEL MECANISMO PARA LA RECUPERACIÓN Y RESILENCIA – NEXT GENERATION EU EN EL MARCO DEL COMPONENTE 5 "PRESERVACIÓN DEL LITORAL Y RECURSOS HÍDRICOS" INVERSIÓN 3 (C5.I3) DENOMINADA «TRANSICIÓN DIGITAL EN EL SECTOR DEL AGUA»

Este documento describe las especificaciones técnicas mínimas para la adquisición, instalación y mantenimiento de soluciones de seguridad perimetral (firewalls), switches de acceso, una plataforma de gestión centralizada, un sistema de registro y analítica de seguridad y una plataforma NAC para **26 Plantas (ETAP/EDAR)** y **13 Oficinas remotas** para el Despliegue del Plan de Ciberseguridad incluido en la actuación A21 del proyecto TRADIGUSA.

Creación y configuración de VLAN en todas las sedes

1. El adjudicatario deberá definir, crear y dejar operativas un mínimo de **cinco (5) VLAN** en cada una de las 39 sedes (26 plantas + 13 Oficinas).
2. Para cada VLAN se configurará:

    - Etiqueta 802.1Q coherente en switches y firewalls.
    - Pasarela de capa 3 (SVI o sub-interfaz) con direccionamiento IP facilitado por la propiedad.
    - Políticas de acceso en el firewall de acuerdo con el esquema de seguridad (permitir, denegar o inspeccionar tráfico entre VLAN).
    - QoS/DSCP adecuado: priorización de Voz (VLAN 20) y limitación de ancho de banda en Invitados (VLAN 30).
    - DHCP relay o servidor local, según diseño.

3. El licitador aportará plantillas para el Manager que permitan la réplica automática de las 5 VLAN y sus políticas en nuevas sedes.
4. Las VLAN deberán quedar operativas y verificadas durante las pruebas de aceptación, demostrando:

    - Conectividad intra-VLAN (L2) y entre VLAN autorizadas (L3).
    - Aplicación correcta de políticas de firewall y QoS.

    - Toda la configuración se documentará en el "Libro de red" entregado al finalizar la implantación (diagramas, rangos IP, ACL, rutas).

5. Toda la configuración se documentará en el "Libro de red" entregado al finalizar la implantación (diagramas, rangos IP, ACL, rutas).

SECCIÓN I: ESPECIFICACIONES PARA FIREWALLS EN 26 PLANTAS (ETAP/EDAR)

Objeto del Contrato: Suministro, instalación y mantenimiento de una **solución de alta disponibilidad (HA)** compuesta por **dos (2) dispositivos** de seguridad perimetral por cada una de las 26 plantas para el Despliegue del Plan de Ciberseguridad incluido en la actuación A21 del proyecto TRADIGUSA. La función principal de la solución será la segmentación estricta y la protección de la red local de la planta, controlando el tráfico entre las zonas de Tecnología de la Información (TI) y Tecnología de Operación (OT), y gestionando la conectividad segura hacia la sede central a través de la red MPLS.

1. Especificaciones del Hardware y Rendimiento Mínimo

El licitador deberá adjuntar la ficha técnica oficial del fabricante, incluyendo una tabla de conformidad donde se destaquen en negrita los valores medidos de: Firewall (UDP 1518B), Protección contra Amenazas (Threat Protection), Inspección SSL/TLS 1.3, Rendimiento IPS, Sesiones concurrentes y CPS.

1.1. Formato y Puertos:

- Formato de **sobremesa o enracable**.
- Cada dispositivo deberá disponer de un mínimo de **5 puertos físicos 1 Gbps (10/100/1000 Mbps) RJ45**.

1.2. Memoria RAM

- Memoria RAM mínima: Cada dispositivo deberá disponer de una memoria RAM mínima de **4 GB**.

1.3. Rendimiento de Red y Seguridad (Valores Mínimos por Dispositivo):

- Rendimiento de Firewall (UDP 1518B): **≥ 5 Gbps**.
- Rendimiento de Protección contra Amenazas (Threat Protection, con IPS, Control de Aplicaciones y Antivirus activados): **≥ 900 Mbps**.
- Rendimiento IPS (solo motor IPS): **≥ 1.5 Gbps**.
- Inspección SSL/TLS 1.3 (descifrado+IPS+re-cifrado): **≥ 800 Mbps**.

- Sesiones Concurrentes (TCP): **≥ 1,100,000**.
- Nuevas Sesiones por Segundo (TCP): **≥ 45,000**.

1.4. Alta Disponibilidad (HA):

- La solución deberá soportar de forma nativa configuraciones de alta disponibilidad en modo **Activo-Pasivo (obligatorio)** y **Activo-Activo (opcional)**, sin requerir licencias de software adicionales ni costes extra para habilitar y operar esta funcionalidad.

2. Funcionalidades Específicas de Seguridad (OT/ICS)

La oferta deberá incluir un paquete de seguridad centrado en OT activo durante todo el contrato, que cumpla con:

2.1. Visibilidad y Descubrimiento Pasivo de Activos OT: Capacidad para descubrir, identificar y clasificar los activos en la red OT (PLCs, HMIs, RTUs, etc.) sin realizar escaneos activos.

2.2. Inspección Profunda de Protocolos (DPI) Industriales: Soportar de forma nativa la decodificación e inspección de, como mínimo, los siguientes protocolos: Modbus/TCP, S7 Communication, EtherNet/IP (CIP), DNP3, OPC UA, y Profinet.

2.3. Políticas Contextuales para OT: Permitir la creación de políticas de firewall granulares basadas en el contexto OT, permitiendo o denegando acciones específicas dentro de un protocolo.

2.4. Firmas de Vulnerabilidades para ICS: El servicio de IPS deberá incluir un conjunto de firmas específico y actualizado para detectar vulnerabilidades en sistemas de control industrial.

3. Funcionalidades de Red

3.1. Segmentación de Red: Soporte nativo IEEE 802.1Q para al menos 10 VLANs, con políticas de firewall stateful entre ellas.

3.2. Conectividad Segura (VPN): Soporte IPsec (IKEv1/v2) para la conexión a la sede central.

4. Gestión, Soporte y Mantenimiento

4.1. Gestión y Administración: Interfaz gráfica web intuitiva (español/inglés) y capacidad de gestión centralizada desde la plataforma del fabricante.

4.2. Soporte y Mantenimiento:

- Contrato de soporte del fabricante por un periodo de **5 años**, que incluya las licencias necesarias para las funcionalidades descritas (especialmente IPS y OT Security).
- Soporte técnico **24x7x365**.
- Sustitución avanzada de hardware (NBD - Next Business Day).
- Acceso a todas las actualizaciones de firmware y firmas de seguridad durante el contrato.

SECCIÓN II: ESPECIFICACIONES PARA FIREWALLS EN 13 OFICINAS

Objeto del Contrato: Suministro, instalación y mantenimiento de una **solución de alta disponibilidad (HA)** compuesta por **dos (2) dispositivos** de seguridad perimetral por cada una de las 13 oficinas remotas. La función principal del equipo será la segmentación de la red local, la gestión de la conectividad segura hacia la sede central y la priorización del tráfico de voz.

1. Especificaciones del Hardware y Rendimiento Mínimo

El licitador deberá adjuntar la ficha técnica oficial del fabricante, incluyendo una tabla de conformidad donde se destaquen en negrita los valores medidos de: Firewall (UDP 1518B), Protección contra Amenazas (Threat Protection), Inspección SSL/TLS 1.3, Rendimiento IPS, Sesiones concurrentes y CPS.

1.1. Formato y Puertos:

- Formato **sobremesa o enracable**, diseño **fanless (0 dBA)** para operación silenciosa. Se valorará negativamente la existencia de ventiladores.
- El dispositivo deberá disponer de un mínimo de **5 puertos físicos 1 Gbps (10/100/1000 Mbps) RJ45**.

1.2. Memoria RAM

- Memoria RAM mínima: El dispositivo deberá disponer de una memoria RAM mínima de **4 GB**.

1.3. Rendimiento de Red y Seguridad (Valores Mínimos por Dispositivo):

- Rendimiento de Firewall (UDP 1518B): **≥ 5 Gbps**.

- Rendimiento de Protección contra Amenazas (Threat Protection, con IPS, Control de Aplicaciones y Antivirus activados): **≥ 900 Mbps**.
- Rendimiento IPS (solo motor IPS): **≥ 1.5 Gbps**.
- Inspección SSL/TLS 1.3 (descifrado+IPS+re-cifrado): **≥ 800 Mbps**.
- Sesiones Concurrentes (TCP): **≥ 1,100,000**.
- Nuevas Sesiones por Segundo (TCP): **≥ 45,000**.

1.4. Alta Disponibilidad (HA):

- La solución deberá soportar de forma nativa configuraciones de alta disponibilidad en modo **Activo-Pasivo (obligatorio)** y **Activo-Activo (opcional)**, sin requerir licencias de software adicionales ni costes extra para habilitar y operar esta funcionalidad.

2. Funcionalidades de Red

2.1. Segmentación de Red: Soporte nativo IEEE 802.1Q para al menos 10 VLANs, con políticas de firewall stateful entre ellas.

2.2. Conectividad Segura (VPN): Soporte IPsec (IKEv1/v2) para la conexión a la sede central.

3. Gestión, Soporte y Mantenimiento

3.1. Soporte y Mantenimiento:

- Contrato de soporte del fabricante por un periodo de **5 años**, que incluya las licencias necesarias para las funcionalidades descritas (especialmente IPS y las funciones de seguridad de amenazas avanzadas).
- Soporte técnico **24x7x365**.
- Sustitución avanzada de hardware (NBD - Next Business Day).
- Acceso a todas las actualizaciones de firmware y firmas de seguridad durante el contrato.

SECCIÓN III: ESPECIFICACIONES PARA 39 SWITCHES DE ACCESO GIGABIT

(1 por planta industrial y 1 por oficina de atención al cliente)

1. Objeto

Suministro, instalación y soporte de treinta y nueve (39) switches gestionables de acceso, capa 2+/3-lite, destinados a dar servicio a las 5 VLAN definidas por sede (datos, voz, gestión, invitados y OT).

2. Requisitos mínimos por equipo

El licitador presentará datasheet oficial que acredite todos los valores.

Nº	Concepto	Valor exigido	Motivo / ref.
2.1	Puertos cobre	**≥ 24 × 10/100/1000 Base-T autosensing**	Cobertura a puestos y CCTV
2.2	Uplinks	**≥ 4 × SFP+ 10 GbE (o superiores)**	Troncales a core/SD-WAN
2.3	Switching capacity	**≥ 120 Gb/s dúplex**	FS-124F = 128 Gb/s
2.4	Forwarding rate	**≥ 180 Mpps**	FS-124F = 190 Mpps
2.5	Latencia L2	**< 3 µs**	Garantiza tráfico OT
2.6	Buffers & MAC	**≥ 2 MB buffer • ≥ 16 K MAC**	Evita drops en ráfagas
2.7	VLANs	**≥ 256 VLAN 802.1Q; crear 5 VLAN base por sede**	Segmentación requerida
2.8	LACP	**≥ 8 grupos • ≥ 4 miembros/grupo**	Enlaces agregados
2.9	STP	**RSTP y MSTP (≥ 16 instancias)**	Redundancia capa 2

Nº	Concepto	Valor exigido	Motivo / ref.
2.10	QoS	**8 colas, 802.1p/DSCP, rate-limit por puerto**	Voz y OT
2.11	IGMP Snooping	**v1/v2/v3 + Querier**	Streaming CCTV
2.12	Routing	**≥ 16 rutas estáticas (IPv4/IPv6)**	Separación básica
2.13	Seguridad	**802.1X, MAC-Auth Bypass, ACL por VLAN/puerto**	Integración con NAC
2.14	Gestión	**CLI + Web + SNMP v2/v3 + Syslog + REST API**	Multi-fabricante
2.15	Consumo y ruido	**Fanless • ≤ 20 W típico**	Armario de planta
2.16	Dimensiones	**1 U, montaje rack 19”**	Estándar
2.17	Certificaciones	**CE, FCC, RoHS**	Conformidad

3. Licencias y soporte (5 años)

Concepto	Exigencia
Soporte	**24 × 7 HW + SW con recambio NBD**
Firmware	**Acceso a actualizaciones durante los 5 años**
Gestión	**Integración con la plataforma de red elegida sin costes ocultos**

4. Pruebas de aceptación

Prueba	Criterio
VLANs	**Creación y paso de tráfico en las 5 VLAN base**
Throughput L2	**Tramas de 1518 B a línea 1 Gb/s en todos los puertos sin pérdidas**
Agregación LACP	**Impar/recuperación < 2 s en un grupo 2 × 10 Gb**
Latencia	**< 3 µs promedio puerto-puerto (25 °C)**

5. Verificación y concurrencia

El licitador presentará datasheet oficial que acredite todos los valores del apartado 2. Se admitirá cualquier switch que cumpla o supere las especificaciones.

SECCIÓN IV: ESPECIFICACIONES PARA PLATAFORMA DE GESTIÓN CENTRALIZADA DE SEGURIDAD (MANAGER)

1. Objeto

Suministro, implantación y soporte de una plataforma de gestión centralizada (física, virtual o SaaS) capaz de administrar los 78 cortafuegos NGFW/SD-WAN (52 para plantas y 26 para oficinas), los 39 switches de acceso y demás dispositivos de la red corporativa, con automatización de despliegues, control de versiones y alta disponibilidad.

2. Requisitos mínimos

Nº	Concepto	Requisito mínimo
2.1	Modalidad	**Appliance físico, virtual (VMware/Hyper-V/KVM) o SaaS respaldado por el fabricante**
2.2	Capacidad de gestión	**≥ 150 dispositivos (firewalls/VDOM, switches, AP)**

Nº	Concepto	Requisito mínimo
2.3	Administradores concurrentes	**≥ 10 con RBAC granular**
2.4	Alta disponibilidad	**Cluster activo-pasivo sin licencias adicionales; fail-over ≤ 5 min**
2.5	Multi-tenant / dominios	**Segmentación lógica por sede con herencia de políticas globales**
2.6	Plantillas y ZTP	**Plantillas reutilizables y Zero-Touch Provisioning para alta automática**
2.7	Versionado & rollback	**≥ 30 versiones almacenadas por dispositivo, comparación y rollback inmediato**
2.8	Distribución de firmware	**Descarga, staging y push programado con validación previa**
2.9	Orquestación SD-WAN	**Definición centralizada de SLA y overlays IPsec/SSL**
2.10	API	**API REST/JSON para CI/CD y automatización externa**
2.11	Seguridad	**MFA obligatorio; soporte SAML/LDAP/RADIUS; cifrado TLS 1.2+ en todas las interfaces**
2.12	Integración SOC	**Exportación de inventario y eventos a SGCES/SIEM vía API o Syslog**

3. Licencias y soporte (5 años)

Concepto	Exigencia
Soporte	**24 × 7 software, actualizaciones y hotfix; recambio hardware si procede**
Capacidad inicial	**Licencia incluida para ≥ 150 dispositivos gestionados**
Actualizaciones software	**Acceso a todas las versiones mayores y menores durante 5 años**

4. Pruebas de aceptación

Prueba	Criterio
Zero-Touch Provisioning	**Alta automática de un firewall sin intervención manual**
Push de plantilla	**Aplicación de cambio a los 78 dispositivos en < 3 min**
Rollback	**Restauración de una versión previa en < 2 min**
Fail-over HA	**Conmutación al nodo pasivo ≤ 5 min con preservación de base de datos**

5. Verificación y concurrencia

El licitador presentará datasheet oficial que acredite todos los valores del apartado 2. Se aceptará cualquier plataforma que iguale o supere estas especificaciones.

SECCIÓN V: ESPECIFICACIONES PARA SISTEMA DE REGISTRO Y ANALÍTICA DE SEGURIDAD (SGCES)

1. Objeto

Suministro, implantación y soporte de un sistema centralizado para la recopilación, almacenamiento, análisis y generación de informes de logs de seguridad procedentes

de los 78 cortafuegos, con capacidad de crecimiento y alta disponibilidad. Este sistema cubrirá las 39 sedes (26 plantas industriales y 13 oficinas de atención al cliente).

2. Requisitos mínimos

Nº	Concepto	Requisito mínimo
2.1	Arquitectura	**Appliance físico o VM endurecida con TPM / Root of Trust; SO dedicado y firmado**
2.2	Ingesta analítica	**≥ 2 000 logs/s de forma sostenida**
2.3	Ingesta modo collector	**≥ 3 000 logs/s**
2.4	Volumen diario	**≥ 100 GB de logs/día con analítica completa**
2.5	Retención on-box	**≥ 30 días a 100 GB/día; RAID-1 o superior con ≥ 8 TB brutos / ≥ 4 TB útiles**
2.6	Dispositivos gestionados	**≥ 150 dispositivos o VDOM simultáneos**
2.7	Interfaces	**≥ 4 × 1 GbE (datos, OOB, HA, expansión)**
2.8	Alta disponibilidad	**Cluster activo-pasivo sin coste de licencias; fail-over ≤ 5 min**
2.9	Exportación	**Reenvío a SIEM externo vía Syslog/CEF (UDP/TCP/TLS) y API REST**
2.10	Analítica	**Búsquedas full-text, dashboards en tiempo real, correlación multi-evento y alertas**

Nº	Concepto	Requisito mínimo
2.11	Cumplimiento	**Plantillas de informes RGPD, ENS, PCI-DSS, ISO 27001**
2.12	Automatización	**API REST/JSON y webhooks para SOAR; playbooks básicos incluidos**

3. Licencias y soporte (5 años)

Concepto	Exigencia
Soporte	**24 × 7 hardware y software, recambio NBD**
Servicios de contenido	**Actualizaciones de firmas/IOC y correlación durante 5 años**
Actualizaciones software	**Acceso a versiones mayores y menores sin coste adicional**

4. Pruebas de aceptación

Prueba	Criterio
Carga de eventos	**Ingesta sostenida de 2 000 logs/s durante 2 h sin pérdida**
Retención	**Verificar almacenamiento de 30 días simulados a 100 GB/día**
Búsqueda	**Respuesta < 5 s a consulta de 24 h de logs**
Fail-over	**Conmutación al nodo pasivo ≤ 5 min con preservación de logs**

5. Verificación y concurrencia

El licitador presentará datasheet oficial que acredite el cumplimiento de todos los puntos del apartado 2. Se aceptará cualquier solución (física, virtual o SaaS) que iguale o supere estos valores.

SECCIÓN VI: ESPECIFICACIONES PARA PLATAFORMA NAC / CONTROL DE ACCESO A RED

1. Objeto

Plataforma NAC virtual o SaaS que proporcione visibilidad, autenticación y micro-segmentación para ≥ 2.500 endpoints concurrentes en la fase inicial, ampliable a ≥ 5.000 endpoints mediante licencias, sin sustitución de hardware. Esta plataforma cubrirá las 39 sedes (26 plantas industriales + 13 oficinas de atención al cliente).

2. Requisitos mínimos

Nº	Concepto	Valor exigido
2.1	Modalidad	**VM (VMware/KVM/Hyper-V) o SaaS del fabricante**
2.2	Escalabilidad	**Licencia inicial ≥ 2.500 EP; ampliable a ≥ 5.000 EP**
2.3	Dispositivos de red	**Gestión de ≥ 150 switches/AP/firewalls**
2.4	Alta disponibilidad	**Cluster activo-pasivo; fail-over ≤ 5 min sin coste extra**
2.5	Métodos de control	**802.1X (EAP-TLS/PEAP), MAB, Captive, SNMP-CoA, VLAN/ACL dinámica**
2.6	Perfilado & visibilidad	**≥ 10 técnicas (DHCP, LLDP, NetFlow, SNMP, ML, etc.) + ≥ 1 M huellas IoT**

Nº	Concepto	Valor exigido
2.7	Postura	**Agente disoluble, agente persistente y modo agent-less**
2.8	Portal BYOD/Invitado	**Personalizable, CA interna, SMS/e-mail OTP**
2.9	Automatización & API	**API REST/JSON + webhooks; integración con SOAR y firewalls**
2.10	Micro-segmentación	**Asignación dinámica de VLAN, VXLAN, SGT o roles**
2.11	Cumplimiento	**Informes RGPD, ENS, PCI-DSS, ISO 27001**
2.12	Multivendor	**Compatibilidad con ≥ 20 fabricantes de switches/AP**

3. Licencias y soporte (5 años)

Concepto	Exigencia
Soporte	**24 × 7 software, actualizaciones y hotfix**
Actualizaciones	**Motores de perfilado, huellas IoT y reglas de política durante 5 años**
Ampliación	**Posibilidad de ampliar licencias por bloques sin reinstalar la plataforma**

4. Pruebas de aceptación

Prueba	Criterio
Perfilado	**Detección automática de PC, cámara IP y PLC S7 en < 60 s**
Autenticación 802.1X	**Puesto Windows con certificado EAP-TLS accede a VLAN Datos**
Micro-segmentación	**PLC aislado en VLAN OT y bloqueado al revocar certificado**
Fail-over HA	**Conmutación ≤ 5 min sin pérdida de base de datos**
Carga	**2.500 EP simultáneos durante 2 h sin degradar respuesta del portal**

5. Verificación y concurrencia

El licitador presentará datasheet oficial que acredite el cumplimiento de todos los valores del apartado 2. Se admitirá cualquier solución que cumpla o supere estas especificaciones.

SECCIÓN VII: CLAUSULAS A CUMPLIR POR TOS LOS EQUIPOS

1. ÁMBITO Y CATEGORÍA ENS

Todos los componentes hardware y software ofertados deberán ser aptos para operar en sistemas sujetos al Esquema Nacional de Seguridad (ENS) en categoría ALTA o MEDIA, según corresponda a cada caso de uso.

2. REQUISITOS DE CONFORMIDAD Y MEDIOAMBIENTALES

- Marcado CE de conformidad con las Directivas:

– 2014/53/UE (RED) o 2014/30/UE (EMC).

- Cumplimiento de la Directiva 2011/65/UE (RoHS II) y del Reglamento (CE) 1907/2006 (REACH).

3. SOLVENCIA TÉCNICA Y PROFESIONAL DEL LICITADOR

a) Experiencia acreditada: al menos **tres (3) suministros** de naturaleza análoga ejecutados en los últimos **cinco (5) años**, cada uno por importe igual o superior al **40 %** del presupuesto de licitación, de los que **uno** deberá corresponder a un organismo público o infraestructura crítica del sector agua o similar.

b) Certificaciones vigentes: ISO 9001 (calidad), ISO 27001 (SGSI) y, si el adjudicatario presta soporte gestionado, ISO 20000-1 (servicios TI).

c) Declaración o Certificado ENS que cubra las actividades de instalación, operación y mantenimiento objeto del contrato.

d) Personal mínimo adscrito al proyecto:

– 1 ingeniero con certificación específica del fabricante del producto ofertado (p. ej. NSE 4/7, PCNSA, ExtremeXOS-SE, etc.).

e) Nivel de partnership con el fabricante que permita acceso a soporte 24×7 y RMA avanzado.

4. DOCUMENTACIÓN A APORTAR EN LA FASE DE LICITACIÓN

• Copia del estado “Cualificado” o “En evaluación” en el CPSTIC (pantalla o certificado CCN).

• Declaraciones UE de conformidad (CE), certificados RoHS II y REACH, y certificados FIPS 140-3 (o equivalentes) de cada modelo.

• Fichas técnicas completas que avalen las especificaciones funcionales exigidas (IPv6, 802.1X, MACsec, PoE, etc.) sólo aplique a los **switches**.

• Relación de suministros principales con certificados de buena ejecución emitidos por los clientes.

• Copia de las certificaciones ISO y del certificado/declaración ENS del licitador.

• Currículos y certificados vigentes del personal propuesto.

5. RÉGIMEN SANCIONADOR

La falsedad, carencia o pérdida de vigencia de cualquiera de las acreditaciones definidas en los apartados anteriores constituirá causa de exclusión de la licitación o, en su caso, de resolución del contrato por incumplimiento culpable del adjudicatario, con incautación de la garantía definitiva y sin perjuicio de las responsabilidades adicionales que procedan.

6. Formación y transferencia de conocimiento

El licitador está obligado a impartir al menos 4 días de formación certificada (presencial u online) para los administradores internos, con entrega de manuales y laboratorios handson.

7. APIs abiertas y documentación

Detalla que todas las interacciones (provisioning, alertas, métricas) deberán ofrecerse vía RESTful JSON con OpenAPI/Swagger documentado, sin capas propietarias inexplicables.