

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL
SUMINISTRO DE EQUIPAMIENTO DE COMUNICACIONES Y DE SEGURIDAD, Y
RENOVACIÓN DEL SOPORTE DEL EQUIPAMIENTO EXISTENTE EN LA AGENCIA
ANDALUZA DE INSTITUCIONES CULTURALES

CONTR2025 0000580405

Ntra. Ref: E25-001718

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 1 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



Índice

1. Introducción	3
2. Objeto del contrato	4
2.1. Lote 1: Suministro e instalación de nueve switches de planta y dos switches de core incluyendo soporte, y material auxiliar de conexión e instalación.	4
2.2. Lote 2: Suministro, instalación y configuración de un dispositivo Fortianalyzer con soporte premium incluido.	7
2.3. Lote 3: Ampliación del soporte y garantía de la infraestructura del fabricante Fortinet.....	7
Definición de las condiciones a las que deberá ajustarse la ejecución del suministro	7
3. Condiciones generales de realización	8
3.1. Instalación y puesta en marcha	8
Lote 1: Suministro e instalación de nueve switches de planta y dos switches de core incluyendo soporte, y material auxiliar de conexión e instalación.	8
Lote 2: Suministro, instalación y configuración de un dispositivo Fortianalyzer con soporte enterprise incluido.....	9
Lote 3: Ampliación del soporte y garantía de la infraestructura del fabricante Fortinet.	10
3.2. Propiedad Intelectual del Resultado de los Trabajos	10
3.3. Confidencialidad de la Información.....	10
3.4. Cumplimiento del Esquema Nacional de Seguridad.....	10
3.4.1. Colaboración en la gestión de la seguridad del sistema.....	11
3.4.2. Certificación ENS de la empresa licitadora	11
3.4.3. Certificación ENS de la empresa licitadora	12
3.4.4. Punto de contacto (POC) de seguridad	12
3.4.5. Gestión de incidentes.....	12
3.4.6. Accesos remotos.....	12
3.5. Protección de datos y garantía de los derechos digitales.....	13
4. Lugar y plazo de entrega.....	13
5. Responsable del contrato	14
6. Garantía.....	15

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 2 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



1. INTRODUCCIÓN

La Agencia Andaluza de Instituciones Culturales (en adelante la Agencia), es una agencia empresarial de las previstas en la letra b) del apartado 1 del artículo 68 de la Ley 9/2007, de 22 de octubre, de Administración de la Junta de Andalucía.

Tiene como objetivo el optimizar, en términos de eficacia y economía, la gestión de los recursos públicos que la Administración de la Junta de Andalucía destina a la cultura, así como aquellos recursos obtenidos en el ejercicio de su actividad como consecuencia de la prestación de bienes y servicios que se entreguen o realicen, contribuyendo al acceso a los bienes culturales en condiciones de igualdad, y la participación equitativa de las personas, mujeres y hombres, en las actividades culturales.

La Agencia, lleva a cabo las tareas técnicas y de gestión requeridas para el desarrollo y ejecución de las funciones descritas en el artículo 6 de sus Estatutos y de cuantas otras se le atribuyan, mediante la dirección, organización, producción, fomento, promoción, difusión y divulgación de programas, instituciones, equipamientos e instalaciones culturales.

El equipamiento tecnológico de la Agencia juega un papel importante como herramienta de apoyo al desarrollo de las funciones descritas anteriormente. En la infraestructura de servidores de la Agencia se sustentan todos los servicios corporativos y sistemas de información que son a su vez herramientas de trabajo esenciales para el desarrollo de cualquier actividad de la organización; por tanto, tienen carácter crítico para la misma, según se establece en el análisis de riesgos de los sistemas de información a los que es de aplicación el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Para mantener la infraestructura anterior en un nivel alto de seguridad, la Agencia necesita mantener actualizados los dispositivos de comunicaciones que articulan sus redes informáticas, por lo que requiere la renovación de los dispositivos de red que van quedando obsoletos por otros que permitan aumentar el nivel de seguridad.

En ese sentido, la Agencia utiliza, entre otras medidas, dispositivos de seguridad perimetral (o firewalls) del fabricante Fortinet para proteger sus redes informáticas de accesos no autorizados, la seguridad que proporcionan estos dispositivos depende, entre otros factores, de su nivel de actualización, por lo que es necesario mantener activa la suscripción al soporte del fabricante que da acceso a dichas actualizaciones de seguridad.

Para completar la arquitectura de seguridad de la Agencia, junto a los elementos anteriores (cortafuegos y dispositivos de red), es necesario contar con un dispositivo específico para la recopilación y análisis de eventos de seguridad que incluya la capacidad de reacción automatizada. Dicho dispositivo debe integrarse con los cortafuegos para poder automatizar la respuesta ante ataques y evitar incidentes.

El presente pliego establece los requisitos mínimos que deben cumplir las ofertas presentadas por los licitadores.

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 3 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



2. OBJETO DEL CONTRATO

Constituyen el objeto del presente pliego los siguientes lotes:

2.1.Lote 1: Suministro e instalación de nueve switches de planta y dos switches de core incluyendo soporte, y material auxiliar de conexión e instalación.

Se trata de switches que permitan extender la seguridad del firewall hasta los puntos de conexión de cada equipo de la red, por lo que deben ser compatibles con los cortafuegos existentes en la Agencia.

Por un lado, se requieren 9 switches de planta y, por otro, 2 switches centrales (de “core”) para la distribución desde el CPD de los servicios centrales.

- **Switches de planta:**

Nueve (9) switches de 48 puertos RJ45 1GE y 4 puertos 10GE SFP+, similares a los ya existentes en la Agencia, para homogeneizar la gestión de la red. Cada uno debe incluir, como mínimo, las siguientes características y funcionalidades:

- 48 Puertos 1 GbE RJ45
- 4 Puertos 10 GbE SFP+
- 1 RU de altura como máximo.
- Capacidad de conmutación (dúplex): 176 Gbps
- Paquetes por segundo (dúplex): 260 MPPS
- MAC Address Storage: 32 K
- Latencia de red: Inferior a 1 μ s
- VLANs soportadas: 4K
- Posibilidad de montaje apilado o “en stack”, para que funcionen como una única unidad (En un apartado más adelante de este documento se detallarán los elementos de interconexión necesarios)
- Puerto de consola para administración.
- Capacidad de agrupación de puertos o “Link aggregation”.
- Deben cumplir los siguientes estándares y protocolos:
 - Spanning Tree IEEE 802.1D
 - Autenticación de red IEEE 802.1X
 - VLANs IEEE 802.1Q
 - Prioridad IEEE 802.1p
 - SNMPv3
- Debe incluir soporte del fabricante durante un periodo mínimo de 3 años y garantía de por vida.
- Compatibilidad IPv4 e IPv6
 - Unicast/Multicast
 - 802.1Q Vlan
 - LACP para la agregación de puertos.
- Gestión y administración
 - Posibilidad de volver a una configuración anterior (Rollback)
 - Capacidad de gestión a través de línea de comandos o “CLI”. Tanto a través del puerto de consola como remotamente, a través de SSH.
 - Posibilidad de exportar e importar la configuración en un archivo
 - Soporte de SNMP.
 - Exportación de logs mediante FTP, SCP y/o TFTP
- Registro de, al menos, los siguientes tipos de eventos:
 - 802.1Q VLAN
 - LACP para la agregación de puertos.
 - DHCP Snooping

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 4 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



- IP Source Guard
 - DAI Dynamic ARP Inspection
 - Calidad de servicio (QoS): Tanto por colas (Queue Traffic Shaping) como por puerto (Port Traffic Shaping).
 - Posibilidad de gestionar a través de una consola centralizada que unifique seguridad en la capa de acceso con la seguridad a nivel 3, 4 y 7, con acceso mediante RADIUS.
 - Monitorización de tráfico vía SPAN y RemoteSPAN (nivel 2).
 - Capacidad de detección automática de los dispositivos conectados en cada puerto. Cada switch alimentará de forma automática la base de datos de dispositivos de los cortafuegos mediante integración nativa del propio fabricante.
 - Capacidad de aplicar políticas de NAC y acciones automatizadas en función de eventos de seguridad, en combinación con la plataforma de seguridad según lo descrito anteriormente.
- **Switches de core:**
- Dos (2) switches de 48 puertos 25G/10G/1G SFP28/SFP+/SFP para la distribución a las distintas plantas.** Cada uno debe incluir, como mínimo, las siguientes características y funcionalidades:
- 48 puertos 25G/10G/1G SFP28/SFP+/SFP
 - 2 puertos 10G/1G SFP+/SFP
 - 8 puertos 100G/40G QSFP28/QSFP+
 - 1 RU de altura como máximo.
 - Capacidad de conmutación (dúplex): 4000 Gbps
 - Paquetes por segundo (dúplex 64 bytes): 4000 Mpps
 - MAC Address Storage: 96 K
 - Latencia de red: Inferior a 1 μ s
 - VLANs soportadas: 4K
 - Posibilidad de montaje apilado o “en stack”, para que funcionen como una única unidad (En un apartado más adelante de este documento se detallarán los elementos de interconexión necesarios)
 - Doble fuente de alimentación para redundancia.
 - Puerto de consola para administración.
 - Capacidad de agrupación de puertos o “Link aggregation”.
 - Deben cumplir los siguientes estándares y protocolos:
 - Spanning Tree IEEE 802.1D
 - Autenticación de red IEEE 802.1X
 - VLANs IEEE 802.1Q
 - Prioridad IEEE 802.1p
 - SNMPv3
 - Debe incluir soporte del fabricante durante un periodo mínimo de 3 años y garantía de por vida.
 - Compatibilidad IPv4 e IPv6
 - Unicast/Multicast
 - 802.1Q Vlan
 - LACP para la agregación de puertos.
 - Gestión y administración
 - Posibilidad de volver a una configuración anterior (Rollback)
 - Capacidad de gestión a través de línea de comandos o “CLI”. Tanto a través del puerto de consola como remotamente, a través de SSH.
 - Posibilidad de exportar e importar la configuración en un archivo
 - Soporte de SNMP.
 - Exportación de logs mediante FTP, SCP y/o TFTP
 - Registro de, al menos, los siguientes tipos de eventos:
 - 802.1Q VLAN

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 5 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



- LACP para la agregación de puertos.
- DHCP Snooping
- IP Source Guard
- DAI Dynamic ARP Inspection
- Calidad de servicio (QoS): Tanto por colas (Queue Traffic Shaping) como por puerto (Port Traffic Shaping).
- Posibilidad de gestionar a través de una consola centralizada que unifique seguridad en la capa de acceso con la seguridad a nivel 3, 4 y 7, con acceso mediante RADIUS.
- Monitorización de tráfico vía SPAN y RemoteSPAN (nivel 2).
- Capacidad de detección automática de los dispositivos conectados en cada puerto. Cada switch alimentará de forma automática la base de datos de dispositivos de los cortafuegos mediante integración nativa del propio fabricante.
- Capacidad de aplicar políticas de NAC y acciones automatizadas en función de eventos de seguridad, en combinación con la plataforma de seguridad según lo descrito anteriormente.
- Elementos de interconexión e instalación:
 - Diez (10) Transceptores 10GE SFP+ Multimodo certificados para los switches anteriores
 - Ocho (8) Transceptores 10GE SFP+ Monomodo certificados para los switches anteriores
 - Veintidós (22) cables DAC 10 GE SFP+ de 1 metro de longitud certificados para los switches anteriores
 - Dos (2) cables DAC 100 GE QSFP28 de 1 metro de longitud certificados para los switches anteriores
 - Cuatro (4) latiguillos SFP+ Multimodo de 30 metros de longitud para los transceptores anteriores

Al tratarse de un servicio crítico para la seguridad de la organización, se requiere la adquisición de todo el equipamiento con el soporte incluido (formato “bundle”) durante, al menos, tres años con el fin de garantizar que el equipamiento tenga un funcionamiento óptimo, se mantenga actualizado en todo momento y, en el caso de avería, pueda ser reparado o sustituido a la mayor brevedad posible.

Por otro lado, dentro del alcance de este lote se incluye la configuración e instalación de estos dispositivos tal y como se detalla en el apartado [3.1. Instalación y puesta en marcha](#) de este documento.

Se requiere que el técnico encargado de dicha instalación esté al menos la certificación Fortinet Network Security Professional NSE 4, dado que los equipos suministrados se deberán integrar en la infraestructura existente en la organización.

La seguridad perimetral en las redes informáticas de la Agencia está basada en cortafuegos del fabricante Fortinet, por lo que los dispositivos ofertados deben integrarse con estos dispositivos de seguridad de dicho fabricante para la gestión centralizada de la red LAN, así como para la securización de la misma. Utilizar conmutadores de otro fabricante añade una complejidad adicional a la hora de gestionar las políticas de seguridad con estos equipos, pues en la actualidad se lleva a cabo de forma centralizada. Cualquier complejidad adicional puede derivar en un riesgo de seguridad añadido que se desea evitar.

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 6 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



2.2.Lote 2: Suministro, instalación y configuración de un dispositivo Fortianalyzer con soporte premium incluido.

Para cumplir con la normativa del Esquema Nacional de Seguridad en lo que se refiere a disponer de sistemas que permitan almacenar los logs de eventos de la infraestructura tecnológica, analizar y relacionar esos eventos detectando posibles riesgos de seguridad, así como automatizar determinados procesos para mitigar estos riesgos, la Agencia tiene implantado el dispositivo Fortianalyzer modelo 300G. Dado que este sistema es un elemento crítico para la organización para la gestión de la seguridad de la infraestructura TIC, necesita otro dispositivo para que actúe de respaldo del actual, y se pueda garantizar de forma continua dicho servicio.

Por otro lado, para facilitar la gestión y mitigación de forma automática de posibles riesgos de seguridad, se requiere una suscripción para la descarga de playbooks o plantillas del fabricante Fortinet en las que viene de forma preconfigurada estos comportamientos y que se añadirán o adaptarán a las políticas y medidas que la Agencia tenga particularizada para su organización.

Al tratarse de un servicio crítico para la seguridad de la organización, se requiere la adquisición con el soporte incluido (formato “bundle”) durante, al menos, tres años con el fin de garantizar que el equipamiento tenga un funcionamiento óptimo, se mantenga actualizado en todo momento y, en el caso de avería, pueda ser reparado o sustituido a la mayor brevedad posible.

Además, se incluye el servicio de instalación y configuración de dicho dispositivo en paralelo con el existente para que pueda garantizar la continuidad del servicio en el caso de fallo de uno de ellos. En el alcance de la configuración de dicho equipo se deberá contar con una persona con conocimientos necesarios para que el dispositivo se integre en la infraestructura de la organización y despliegue sus capacidades para la detección y respuesta frente a posibles ataques. Dicha configuración deberá contar con el visto bueno de la persona responsable del contrato. Se valorará como mejora que el perfil propuesto cuente con certificaciones del fabricante para realizar este trabajo.

2.3.Lote 3: Ampliación del soporte y garantía de la infraestructura del fabricante Fortinet.

Renovación, durante 3 años, del soporte de doce (12) cortafuegos instalados en la Agencia, para proteger las redes de los distintos centros de la organización frente a ataques informáticos que puedan poner en riesgo la seguridad de la infraestructura tecnológica e información de la Agencia.

Definición de las condiciones a las que deberá ajustarse la ejecución del suministro

En este apartado se detallan las características del soporte a renovar. Las características mínimas que debe incluir el soporte son las siguientes:

- AntiVirus
- IPS
- Web Filtering
- Email Filtering
- Outbreak Protection

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 7 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



Para los siguientes dispositivos (números de serie) y fechas de fin de soporte actuales:

Modelo	Número de serie	Fecha fin soporte actual
FortiGate 201F	FG201FT922921208	25/05/2026
FortiGate 201F	FG201FT922921214	25/05/2026
FortiGate 60F	FGT60FTK20030215	25/05/2026
FortiGate 60F	FGT60FTK20029913	25/05/2026
FortiGate 60F	FGT60FTK20033164	25/05/2026
FortiGate 60F	FGT60FTK20035995	25/05/2026
FortiGate 60F	FGT60FTK20030116	25/05/2026
FortiGate 60F	FGT60FTK20029917	25/05/2026
FortiGate 60F	FGT60FTK2209JSLM	25/05/2026
FortiGate 60F	FGT60FTK2209JSS0	25/05/2026
FortiGate 60F	FGT60FTK2209JKLM	25/05/2026
FortiGate 60F	FGT60FTK2209JSJJ	25/05/2026

Además, se deberá renovar la suscripción del dispositivo virtual para la gestión centralizada de los cortafuegos (FortiManager), el cual tiene como fecha de caducidad el 22 de mayo de 2026.

3.CONDICIONES GENERALES DE REALIZACIÓN

La mera presentación de propuestas implica la aceptación sin reservas por parte del licitador y, en todo caso, por el adjudicatario de las condiciones establecidas en los Pliegos que rigen la presente contratación.

El adjudicatario realizará todos los trabajos necesarios destinados a conseguir los objetivos fijados en este documento. Como resultado final, la Agencia Andaluza de Instituciones Culturales habrá de tener datos fehacientes de la correcta realización del suministro solicitado.

3.1. Instalación y puesta en marcha

La instalación y puesta en marcha correrá a cargo del adjudicatario, según las especificaciones de cada lote.

Lote 1: Suministro e instalación de nueve switches de planta y dos switches de core incluyendo soporte, y material auxiliar de conexión e instalación.

La instalación y configuración de estos elementos corresponderá al adjudicatario, según la siguiente distribución en las distintas sedes de la Agencia:

Elemento	Sede	Dirección	Interconexión
2 x Switches de core	Servicios Centrales AAIICC	Estadio La Cartuja, puerta 13, Sevilla (41092)	2 x cables DAC 100 GBE 10 x cables DAC 10 GBE 6 x transceptores multimodo 1 x transceptor monomodo 4 x latiguillos SFP+ 30m
3 x Switches de planta	Centro Andaluz de la Fotografía	C/ Pintor Díaz Molina 9, Almería (04002)	2 x cables DAC 10 GBE 4 x transceptores multimodo



2 x Switches de planta	Edificio Rey Chico	Paseo de los Tristes s/n. Edificio Rey Chico, Granada (18010)	2 x cables DAC 10 GBE
1 x Switch de planta	Teatro Alhambra	C/ Molinos 56, Granada (18009)	
2 x Switches de planta	Teatro Cánovas	Plaza de El Ejido 5, Málaga (29013)	2 x cables DAC 10 GBE
1 x Switch de planta	Centro Andaluz de las Letras	C/ Álamos 24, Málaga (29012)	

La instalación y configuración de estos elementos podrá requerir modificaciones en la configuración de los cortafuegos de cada sede para asegurar la correcta integración de ambos elementos. Dichas modificaciones también correrán a cargo del adjudicatario.

Por otra parte, al instalar estos switches en cada sede, el adjudicatario debe retirar (y entregar a la Agencia para su almacenamiento) los que venían prestando servicio hasta ese momento por lo que, en los nuevos switches, deben quedar todos los puertos totalmente configurados y parcheados, con las mismas VLANs y parámetros necesarios para la conexión de los equipos, que tenían los switches sustituidos. Es decir, al finalizar la instalación de estos nuevos switches, todos los equipos de las sedes afectadas deben mantener la misma conexión a la red LAN que tuvieron previamente al cambio.

Los parcheos de cada equipo deben quedar documentados tras el cambio, incluyendo:

- Nombre del switch
- Puerto del switch
- VLAN
- Tipo de conexión a la VLAN (Native, tagged, etc.)
- Código de roseta (o conexión directa)
- Nombre del usuario o dispositivo

Los elementos a suministrar que no aparecen en el listado anterior se entregarán en los Servicios Centrales de la Agencia y no requerirán instalación por parte del adjudicatario, tal como se detalla en el apartado correspondiente (Punto 4, Lugar y plazo de entrega).

Lote 2: Suministro, instalación y configuración de un dispositivo Fortianalyzer con soporte enterprise incluido.

La instalación y configuración del Fortianalyzer corresponderá al adjudicatario según las siguientes especificaciones:

- Instalación y puesta marcha del hardware en los servicios centrales de la Agencia en la puerta 13 del Estadio de la Cartuja. 41092 de Sevilla.
- En colaboración con el departamento de sistemas y telecomunicaciones de la Agencia, deberá configurar el equipamiento para que pueda operar con el otro dispositivo del mismo modelo existente.
- En colaboración con el departamento de sistemas y telecomunicaciones de la Agencia, llevará a cabo la configuración necesaria para que pueda operar con normalidad en la infraestructura tecnológica de la Agencia.
- En colaboración con el responsable de seguridad de la organización, se diseñarán e implantarán las capacidades que tienen estos dispositivos para la detección y mitigación de amenazas que detecte en la infraestructura tecnológica de la Agencia, y así como la configuración de la suscripción de los servicios añadidos para el mantenimiento y actualización de plantillas (playbooks).

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 9 / 15
VERIFICACIÓN	NjyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



Lote 3: Ampliación del soporte y garantía de la infraestructura del fabricante Fortinet.

La renovación del soporte corresponderá al adjudicatario.

3.2. Propiedad Intelectual del Resultado de los Trabajos

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente suministro serán propiedad de la Junta de Andalucía, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos. El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente suministro pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la Junta de Andalucía. Específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación corresponden únicamente a la Junta de Andalucía.

3.3. Confidencialidad de la Información

El adjudicatario se obliga a guardar el debido sigilo profesional de cuanta información tenga conocimiento para cumplimiento del presente suministro, tratará los datos conforme a las instrucciones de esta Agencia y no los aplicará o utilizará con fin distinto, ni los comunicará o cederá, ni siquiera para su conservación, a otras personas.

3.4. Cumplimiento del Esquema Nacional de Seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información dictados por el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad.

En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación. Para lograr esto, se adoptarán las medidas de seguridad indicadas en el anexo II del ENS aplicables a la categoría del sistema y a los niveles de seguridad requeridos para el mismo, en las dimensiones de confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad, que se detallan a continuación:

Dimensión de seguridad	Valor
Confidencialidad	Bajo
Integridad	Bajo
Trazabilidad	Bajo
Autenticidad	Bajo
Disponibilidad	Bajo

A estas medidas se sumarán aquellas medidas adicionales que se definan por el Responsable de Seguridad (artículo 28 del ENS) y aquellas que se añadan en base a análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, a la evaluación de impacto

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 10 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



en la protección de datos (artículo 3.3 del ENS).

El Responsable de Seguridad trasladará las medidas aplicables a través del Responsable del Contrato durante la ejecución de este.

Deberá también tenerse en cuenta lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la Política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio) y en su desarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada.

Se atenderá también a la normativa interna del organismo contratante en materia de ciberseguridad.

El organismo contratante desplegará los medios necesarios para auditar el cumplimiento de la política de seguridad y de los niveles de servicio acordados por parte del contratista, según lo expresado en los documentos de contratación.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional - Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (<http://www.ccn-cert.cni.es/>), así como a las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía y a las indicaciones del Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía.

3.4.1. Colaboración en la gestión de la seguridad del sistema

El adjudicatario colaborará con la realización de los análisis de riesgos que se realicen, que tendrán en cuenta los siguientes aspectos:

- Identificación de los activos relevantes dentro del alcance considerado del Sistema de Información.
- Valoración cualitativa de los activos más valiosos del sistema. La valoración de los activos corresponde a los responsables designados en la política de seguridad del organismo. Para ello se tendrá en cuenta el perjuicio que supondría su degradación.
- Identificación y cuantificación de las amenazas más probables.
- Identificación y valoración de las salvaguardas que protegen de dichas amenazas.
- Identificación y valoración del riesgo residual.

El adjudicatario deberá prestar al organismo la colaboración necesaria durante la realización de auditorías técnicas y de cumplimiento normativo.

3.4.2. Certificación ENS de la empresa licitadora

En cumplimiento de la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad aprobada por Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, el adjudicatario deberá disponer de Declaración o Certificación de Conformidad con el ENS categoría BAJA; para la prestación de los servicios o provisión de las soluciones contempladas en este expediente, en caso de existir en el alcance de esta contratación servicios no prestados desde las instalaciones de la Junta de Andalucía (por ejemplo, servicios prestados desde una nube). Esta Certificación de Conformidad con el ENS debe versar sobre soluciones proporcionadas o servicios prestados por el operador del sector privado que estén relacionadas con las soluciones y servicios que son objeto de contratación del presente expediente, según apartado VII.1 de la Instrucción Técnica de Seguridad citada.

Caso de que el adjudicatario no disponga de la Declaración o Certificación de Conformidad indicada, se le otorgará un plazo máximo de 6 meses para la obtención de ésta, contados a partir de la fecha de

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 11 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



adjudicación/formalización del contrato.

3.4.3. Certificación ENS de la empresa licitadora

Se asignarán los roles relacionados con la seguridad de los sistemas de información, reflejados en el Esquema Nacional de Seguridad y detallados en la guía CCN-STIC 801 (Responsabilidades y Funciones en el ENS).

La interlocución con el adjudicatario en aspectos de seguridad corresponderá al Responsable del Contrato, con la colaboración y con la orientación del Responsable de Seguridad.

Todos estos roles serán identificados e informados, dentro del marco normativo de seguridad establecido en la Junta de Andalucía, desde el inicio del desarrollo del sistema.

3.4.4. Punto de contacto (POC) de seguridad

En cumplimiento del artículo 13 del Real Decreto 311/2022 (Esquema Nacional de Seguridad), el adjudicatario deberá designar un PoC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de ciberseguridad y las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

El adjudicatario deberá comunicar cualquier cambio o sustitución de dicho POC a lo largo de la vida del contrato.

Dicho PoC de seguridad será el propio responsable de Ciberseguridad del contratista, formará parte de su área o tendrá comunicación directa con la misma, y su identificación se comunicará al SOC de la Junta de Andalucía a través del Responsable de Seguridad asignado al sistema.

La comunicación de este PoC incluirá la referencia al contrato en el cual se realiza, su duración estimada, las actividades principales a realizar y los accesos remotos que se prevén.

3.4.5. Gestión de incidentes

El adjudicatario comunicará al personal de ciberseguridad del organismo, en primera instancia, o al Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía cualquier ciberincidente que detecte o del que tenga conocimiento.

Para la gestión de los incidentes de seguridad se seguirá lo dictado en la vigente Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC (<https://juntadeandalucia.es/boja/2018/141/29>). En especial, en el punto 6 (comunicación de incidentes), 8 (comunicación entre organismos y entidades de incidentes y medidas adoptadas), 9 (colaboración con AndalucíaCERT) y 11 (denuncias).

3.4.6. Accesos remotos

El acceso remoto de los técnicos del equipo del proyecto, en el marco del contrato, a los servicios o sistemas de información de la entidad contratante Agencia Digital de Andalucía, se realizará nominalmente mediante el procedimiento aprobado por la Red Corporativa de la Junta de Andalucía (que podrá incluir, a modo de ejemplo, la opción de cliente VPN y/o soluciones de tipo SASE) sin necesidad de disponer de una conexión permanente al Nodo de Interconexión de la Red Corporativa de la Junta de Andalucía (funcionamiento en modo cliente de servicios internos, esto es, conectividad no simétrica), previa autorización por parte del Responsable del Contrato. Caso de que algún software necesario por el adjudicatario para el acceso remoto requiera de suscripción, el adjudicatario se deberá hacer cargo de estos posibles gastos ocasionados.

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 12 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



El modo de acceso será tal que garantice la seguridad de operación y explotación del sistema, así como el objetivo de almacenar y gestionar las solicitudes de servicio e incidencias que se produzcan durante la ejecución del contrato.

El adjudicatario debe realizar las solicitudes de forma individual para cada uno de los técnicos que requieran el acceso remoto, debiendo ser validada cada solicitud por el Responsable del Contrato. Asimismo, deberá comunicar en su caso las bajas eventuales que pudiera producirse durante la vida del contrato.

El adjudicatario debe cumplir con la política de acceso remoto que aplique en el organismo durante todo el periodo de vigencia del contrato, que puede incluir, entre otros aspectos: alta del usuario en el Directorio Corporativo de la Junta de Andalucía, mecanismo de identificación y autenticación robusto empleando el certificado digital de la FNMT, software de la red privada virtual a utilizar, funciones permitidas y datos accesibles desde acceso remoto, tiempo máximo para cerrar sesiones inactivas, activación de los registros de actividad, etc.

Igualmente, el adjudicatario asegurará que la comunicación esté limpia de malware, virus y/o cualquier otro tipo de tráfico malicioso o no deseado.

3.5. Protección de datos y garantía de los derechos digitales

En aplicación de lo regulado en la Disposición Adicional Vigésimo Quinta de la LCSP y el artículo 28 de Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos, en adelante RGPD, y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales, tendrá la condición de encargado del tratamiento respecto a todo los datos personales que se incluyan y se traten en ejecución del objeto del presente encargo.

Conforme al apartado 3 del citado artículo 28 del RGPD el tratamiento que haga el encargado se registrará por un contrato o acto jurídico que regule el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categoría de interesados y las obligaciones y derechos del responsable.

En relación con lo anterior se indica que:

El objeto del encargo es el suministro e instalación de 11 conmutadores de red con su soporte y elementos auxiliares de instalación, un dispositivo para el análisis y detección de amenazas, y la renovación del soporte de 12 cortafuegos y su software de administración.

El tratamiento tendrá una duración según lo especificado en el punto 4 del presente documento. Los datos personales que pueden tratarse dentro del marco del encargo son los siguientes:

- De la Agencia: la razón social, CIF de empresa y datos de persona de contacto.
- Las categorías de los interesados son: personas físicas, incluidas las que representan a personas jurídicas relacionadas con las actividades de la Agencia y trabajadores de la Agencia.

El resto de los derechos y obligaciones de las partes en materia de Protección de Datos de Carácter Personal, que han de ser reguladas conforme al artículo 28.3 RGPD.

4. LUGAR Y PLAZO DE ENTREGA

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 13 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



El lugar de entrega o realización del suministro será la sede en la que se ubicará cada dispositivo, según la siguiente tabla:

Lote	Elemento	Sede	Dirección
Lote 1	2 x Switches de core	Servicios Centrales AAIICC	Estadio La Cartuja, puerta 13, Sevilla (41092)
	2 x cables DAC 100 GBE		
	16 x cables DAC 10 GBE		
	8 x transceptores monomodo		
	6 x transceptores multimodo		
	4 x latiguillos SFP multimodo 30 metros		
	3 x Switches de planta	Centro Andaluz de la Fotografía	C/ Pintor Díaz Molina 9, Almería (04002)
	2 x cables DAC 10 GBE		
	4 x transceptores multimodo		
	2 x Switches de planta	Edificio Rey Chico	Paseo de los Tristes s/n. Edificio Rey Chico, Granada (18010)
	2 x cables DAC 10 GBE		
	1 x Switch de planta	Teatro Alhambra	C/ Molinos 56, Granada (18009)
	2 x Switches de planta	Teatro Cánovas	Plaza de El Ejido 5, Málaga (29013)
2 x cables DAC 10 GBE			
1 x Switch de planta	Centro Andaluz de las Letras	C/ Álamos 24, Málaga (29012)	
Lote 2	Fortianalyzer	Servicios Centrales AAIICC	Estadio La Cartuja, puerta 13, Sevilla (41092)
Lote 3	Soporte	Servicios Centrales AAIICC	Estadio La Cartuja, puerta 13, Sevilla (41092)

En la tabla anterior se incluyen todos los elementos a suministrar en el presente expediente, independientemente de que requieran instalación o no, lo cual se especifica en el apartado correspondiente (Punto 3.1, Instalación y puesta en marcha).

En lo que se refiere al plazo de ejecución, se establece en el apartado 4 de la Memoria Justificativa del presente expediente.

5. RESPONSABLE DEL CONTRATO

De conformidad con el artículo 62 de la LCSP, se nombra responsable del contrato a Sebastián Serrano Rico, jefe del departamento de Sistemas y Telecomunicaciones, o persona en quien delegue, a quien corresponderá supervisar su ejecución, adoptar las decisiones y dictar las instrucciones necesarias con el fin de asegurar la correcta realización de la prestación pactada, así como reforzar el control del cumplimiento de éste y agilizar la solución de los diversos incidentes que puedan surgir durante su ejecución, sin que en ningún caso estas facultades puedan implicar el ejercicio de potestades directivas u organizativas sobre el personal de la empresa contratista.

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 14 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	



6. GARANTÍA

El plazo de garantía es el que se establece en la apartado **número 9** de la **memoria justificativa** que forma parte del presente expediente.

* El presente pliego ha sido redactado por José Damián García González, Director Unidad Tecnología y Sistemas, como se hace constar en diligencia adjunta.

Fdo.: José Ángel Vélez González
DIRECTOR AGENCIA ANDALUZA
DE INSTITUCIONES CULTURALES

Fdo.:
EL ADJUDICATARIO

JOSE ANGEL VELEZ GONZALEZ		11/09/2025 12:17:46	PÁGINA: 15 / 15
VERIFICACIÓN	NJyGwqJbuaG78P66NQjt2D9s3e3Nx4	https://ws050.juntadeandalucia.es/verificarFirma/	