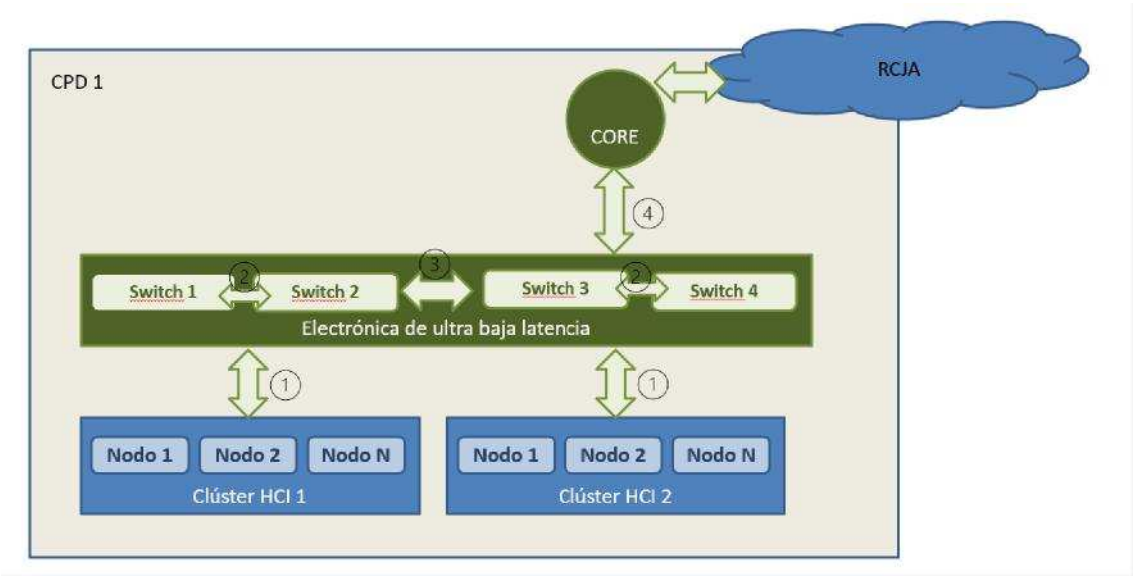
PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO DE INFRAESTRUCTURA DESTINADA A LA AMPLIACIÓN DE LA SOLUCIÓN DE CÓMPUTO Y ALMACENAMIENTO HIPERCONVERGENTE QUE SUSTENTAN LOS SISTEMAS DE INFORMACIÓN UBICADOS EN EL CENTRO DE PROCESAMIENTO DE DATOS PROVINCIAL DE JAÉN.

1. OBJETO DEL CONTRATO

El objeto de la presente contratación lo constituye el suministro de infraestructura destinada a la ampliación de la solución de cómputo y almacenamiento hiperconvergente que sustentan los sistemas de información ubicados en el centro de procesamiento de datos provincial de Jaén, que forma parte de la solución corporativa del Servicio Andaluz de Salud.

En concreto, se requiere el suministro de 1 nodo de cómputo y almacenamiento, y el software necesario para integrarse en las consola de gestión centralizada, que permita ampliar la solución cloud privada hiperconvergente Nutanix, compuesta actualmente por 9 nodos en 1 clúster.

En el Servicio Andaluz de Salud, en cada CPD donde se ubican uno o varios clústeres de la solución de cómputo y almacenamiento hiperconvergente, se cuenta, como parte de ésta, con una infraestructura de comunicaciones compuesta por switches (conmutadores) de ultra baja latencia que se conectan entre sí para dotar de conectividad a los nodos que componen los distintos clústeres de cada CPD entre ellos y hacía otros elementos del CPD, o del exterior al CPD donde se ubican.



Conexión velocidad de enlaces:

1	25 Gbps	4 x nodo
2	100 Gbps	2
3	100 Gbps	4
4	10 Gbps	4

En este contrato se amplía la infraestructura actual de la sede del CPD provincial de Jaén, donde ya existe 1 clúster hiperconvergente y switches de ultra baja latencia.

Así, en base a los requisitos técnicos de los bienes a suministrar, este contrato constará de 1 único lote:

Lote 1	Nodo hiperconvergente para añadir el clúster del CPD provincial de Jaén.

2. ALCANCE DEL SUMINISTRO

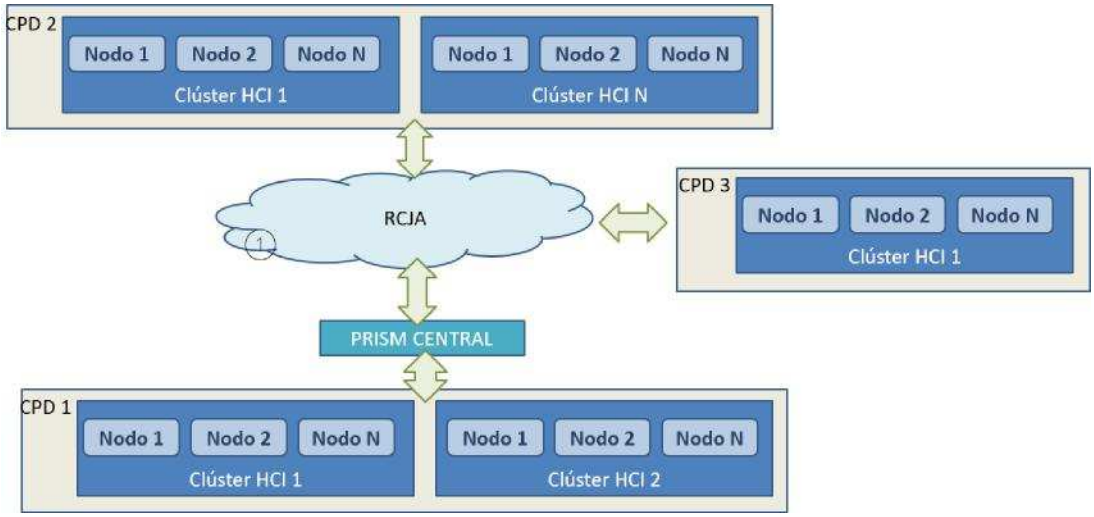
La ampliación de la solución de cómputo y almacenamiento hiperconvergente de los sistemas de información, permitirá la extensión del actual modelo de Centro de Datos Definido por Software Defined Datacenter (SDDC, por sus siglas en inglés) del SAS, que permite que la infraestructura de los Centros de Proceso de Datos (CPD) esté virtualizada y se entregue como servicio; es decir, que dicha infraestructura se gestione de manera remota gobernando la misma a través de una consola automatizada basada en la tecnología Nutanix y denominado PRISM Central.

En este modelo, las funciones de gestión y control se ejercen a nivel software con una interfaz única de monitorización y administración, mientras el hardware, compuesto por nodos, actúa como un banco común de recursos de red, cómputo (CPU, memoria RAM) y almacenamiento (disco), que son asignados en base a las necesidades y cargas de trabajo.

2.1. Descripción de la situación actual de las plataformas hiperconvergentes del SAS

En la actualidad, el SAS dispone de una solución de cómputo y almacenamiento hiperconvergente gobernado mediante el PRISM CENTRAL desde el que se gestiona la infraestructura de red, cómputo y almacenamiento. Dicha solución se apoya en una infraestructura hiperconvergente (HCI) distribuida en nodos agrupados en clústeres. Estos clústeres se distribuyen entre las sedes de servicios centrales y los nueve (9) hospitales provinciales de referencia que ofrecen, de forma agregada, recursos de: procesamiento (cómputo y

memoria), almacenamiento y red, así como los mecanismos de virtualización, protección del dato y recuperación ante desastres de los sistemas críticos del SAS.



La solución de cómputo y almacenamiento hiperconvergente del SAS está compuesta por 142 nodos repartidos en 23 clústeres distribuidos en los Centros de Procesamiento de Datos (CPD) provinciales, en los nueve hospitales de referencia, y de servicios centrales (SSCC) ubicados en Sevilla y Málaga, del Servicio Andaluz de Salud.

2.1.1. Configuración de la infraestructura hiperconvergente actual en el CPD de Jaén

La infraestructura hiperconvergente en el CPD de Jaén se compone de:

- 1 Clúster hiperconvergente (nodos de cómputo y almacenamiento):
  - Software
    - Nutanix AOS PRO + Add-on Advanced Replication.
    - Hipervisor nativo Nutanix Acropolis Hypervisor (AHV).
    - Nutanix “Prism Central PRO”
  - Hardware
    - Lenovo ThinkAgile Serie HX
- Electrónica de red (switches de ultra baja latencia):
  - Mellanox SN2010 Ethernet Switch for Hyperconverged Infrastructures, dos en cada CPD en HA, con S.O. Onyx.
  - Consola de gestión “Mellanox NEO”.

Cada nodo del clúster tiene cuatro puertos de 25 Gbps que se conectan a los switches. Esta unión se hace mediante cables DAC (Direct Attach Copper).

2.1.2. Elementos a suministrar

Los elementos requeridos para esta contratación son:

· Nodo hiperconvergente, para ampliar el clúster de la solución de cómputo y almacenamiento hiperconvergente existente en el CPD provincial de Jaén.

El número de elementos estimados que se deben incorporar es la siguiente:

DENOMINACIÓN DEL ARTÍCULO	N° DE UNIDADES ESTIMADAS	UBICACIÓN	CLUSTER
Nodo hiperconvergente para añadir el clúster del CPD provincial de Jaén	1	CPD Jaén	ntnxjae01

Todos los elementos que se incorporan incluyen tanto el hardware como el software necesario para su funcionamiento y gestión desde las consolas de administración. En el caso del nodo, de la cloud privada Nutanix denominada Prism Central.

El nuevo nodo hiperconvergente a suministrar por la persona adjudicataria deberán estar certificado en el software HCI Nutanix e integrarse en la consola de gestión centralizada “Prism Central PRO” del mismo fabricante, actualmente desplegada en los Servicios Centrales del SAS, permitiendo tanto la gestión centralizada como local y la replicación de máquinas virtuales (en adelante, MVs) entre los distintos clústeres hiperconvergentes propuestos y existentes.

3. REQUISITOS TÉCNICOS

3.1. Requisitos generales de la ampliación de la solución hiperconvergente Nutanix 3.1.1. Características generales.

La persona adjudicataria suministrará, junto con el hardware, el software requerido (Sistema Operativo, Hipervisor, Capa de Control, ...) para la integración del nuevo nodo en la actual plataforma hiperconvergente del SAS descritas en el apartado 2. ALCANCE DEL SUMINISTRO.

La solución ofertada no impondrá ningún límite al número de usuarios o dispositivos cliente que el equipamiento sea capaz de gestionar.

La infraestructura hiperconvergente se compone de capas hardware y software:

Así, las funciones de gestión y control se ejercen a nivel software, con una interfaz única de control, monitorización y administración, mientras el hardware actúa como un banco común de recursos que son asignados en base a las necesidades y cargas de trabajo.

La persona adjudicataria suministrará, incluido dentro del precio del nodo hiperconvergente requerido, el producto que permita extender la funcionalidad de la capa de software de la actual Plataforma Hiperconvergente NUTANIX (ver apartado 2.1 Descripción de la situación actual de las plataformas hiperconvergentes del SAS) a la nueva infraestructura hardware adquirida bajo este contrato, que actualmente incluye los siguientes productos en el entorno de producción:

- Nutanix AOS PRO + Add-on Advanced Replication
- Nutanix Acropolis Hypervisor (AHV).
- Nutanix “Prism Central PRO”.

Este producto a suministrar por la persona adjudicataria, para la administración/gestión del nuevo hardware, deberá integrarse en la consola de gestión centralizada “Prism Central PRO”, actualmente desplegada en los Servicios Centrales del SAS. Esto permitirá la operación, administración y configuración centralizada On-premise, permitiendo tanto la gestión centralizada como la replicación de MVs entre distintos clústeres hiperconvergentes existentes o futuros.
La configuración propuesta debe permitir albergar Prism Central en el clúster propuesto, por lo que dicha configuración debe ser compatible con este fin. Todos los productos se suministrarán en modalidad software-only.

3.2. Requisitos técnicos específicos del suministro del nodo hiperconvergente para la ampliación de la solución de cómputo y almacenamiento hiperconvergente del SAS que sustenta los sistemas de información albergados en el CPD provincial de Jaén.

En la actualidad, el CPD Provincial de Jaén cuenta con un clúster hiperconvergente, siendo necesaria la ampliación de los recursos a través de la incorporación de un nuevo nodo, que quedará gestionados tanto en la capa de control individual del clúster existente como en la capa de control única y centralizada del SAS.

La ampliación se realizará con nodos del mismo fabricante y familia que los nodos que forman la solución de cómputo y almacenamiento hiperconvergente del SAS y que ha quedado descrita en el apartado 2. ALCANCE DEL SUMINISTRO.

En la siguiente tabla se detalla el número de nodos actuales, así como la cantidad de nodos requeridos:

Ubicación	ID	Entorno	Carga de trabajo	Nodos por cluster	
				Actualmente	Requeridos
CPD Jaén	C1	PRO	Propósito general	9	1

Por cuestiones de espacio, operación y mantenimiento, únicamente serán admisibles soluciones que proporcionen todas las especificaciones requeridas del nodo en un único dispositivo, sin elementos o equipos adicionales.

El equipamiento deberá estar certificado con la solución software HCI Nutanix.

Cada nodo dispondrá de las siguientes características físicas:

- Compatible con Rack Standard de 19” existentes en el CPD provincial de Jaén.
- Altura máxima de 2 RU’s dentro del chasis.
- Se debe incluir kit de montaje en rack multifabricante, para su instalación en el rack existente.
- Reemplazo, inserción y retirada “en caliente” (hot swappable) de los elementos replicados: fuentes de alimentación, elementos de ventilación, discos duros; de forma que no haya que interrumpir el sistema eléctrico o interrumpir el servicio, garantizando así una alta disponibilidad.
- Fuentes de alimentación redundantes, sustituibles en caliente y eficientes energéticamente. Cada Fuente de alimentación deberá cumplir:
    - Certificación mínima de nivel de eficiencia energética 80 PLUS White.
- El equipamiento será suministrado para ser alimentado en corriente alterna monofásica, 50Hz, 240V, y permitir la futura ampliación.
- Leds indicadores de estado.
- Cables de alimentación eléctrica (240V, mín. 16A) con conectores C13/C14 en sus extremos.
- Ventiladores redundantes.
- Se proporcionará todo el cableado y conectores necesarios para el funcionamiento del equipo, interconexión y conectividad de éste a la red de datos (cables de corriente, cables de datos, conectores, transceivers, etc.), ajustándose a un diseño de alta disponibilidad.

Las características de rendimiento y capacidad requeridas para el nodo que ampliará el clúster existente del CPD provincial de Jaén son las siguientes:

- Capacidad de proceso:

  - Debe contar, como mínimo, con 2 (dos) procesadores multinúcleo con un número de núcleos físicos por procesador que se describirá más adelante (ver tabla) y que permitan la ejecución concurrente de un mínimo de 2 threads por núcleo (core). La arquitectura de los procesadores debe permitir la conexión directa entre procesadores e integrar el controlador de memoria en el chip del procesador.
  - Los procesadores deben ser x86/64 bits con tecnología integrada que favorezca la virtualización (facilite el cambio de contexto de MVs y optimice procesos de I/O) y proporcione un sistema de ahorro de consumo de energía.
  - Se deberá proveer siempre procesadores de penúltima generación o superior.
  - Cada procesador multinúcleo debe tener una puntuación igual o superior a la que se especificará más adelante (ver tabla) obtenida a través del programa para el cálculo de rendimiento Passmark CPU Benchmark Test V9.
- Memoria RAM:
  - La cantidad de memoria se especificará más adelante en cada clúster. (Ver tabla)
  - La tecnología de memoria será DDR4 a la máxima frecuencia permitida por el equipamiento (en módulos de memoria de la misma capacidad),
  - La distribución de los módulos debe ser balanceada, no se aceptarán configuraciones no balanceadas y que por tanto impacten negativamente en el rendimiento.
  - La distribución de módulos de memoria deberá ocupar como máximo la mitad de los bancos de memoria.
- Almacenamiento:
  - El número, tamaño y tecnología de disco a incluir se describe más adelante. (Ver tabla)
  - Los discos deben ser intercambiables en caliente (hot-plug) de modo que sea posible añadir/reemplazar el disco sin necesidad de apagar el equipo.
  - La solución debe incorporar “tiering” automático en lecturas y escrituras de datos entre los distintos tipos de discos, alojando sobre discos SSD los datos más utilizados (“Hot Data”) y sobre disco rotacional HDD los datos menos accedidos (“Cold Data”).
  - La velocidad de transferencia de los discos SSD, será de, al menos, 6 Gbps o superior.
  - Para optimizar el uso de los discos SSD y el rendimiento de la plataforma, los nodos deberán utilizar los citados discos de SSD desempeñando tanto la función de cache como la de almacenamiento.
  - Incluirá mecanismos de optimización de espacio en disco SSD permitiendo un uso elevado de IOPS, es decir, aplicará técnicas de deduplicación sobre los datos alojados sobre éstos.
  - Incluirá mecanismos de optimización de espacio en discos rotacionales. Estas técnicas de eficiencia serán compresión y deduplicación. Al menos los mecanismos de compresión podrán ser configurados para aplicarse in-line o post-process.
- Discos de arranque
  - Los discos internos destinados al arranque del sistema operativo de los nodos deberán estar redundados.
- Conectividad del nodo:
  - Debe incluir un mínimo de 4 puertos a 25 GbE SFP28 útiles (adicionales a los de gestión remota o consolas).
  - Los puertos de red que se requieren se suministrarán en 2 tarjetas NIC independientes.
  - La solución debe permitir la configuración de las interfaces en modo agregado, mediante protocolo 802.3ad (LACP).
  - Debe incluir, al menos, 1 puerto 10/100/1000 Mb Ethernet Base-T para la gestión fuera de banda.
  - Debe incluir un mínimo de 1 Puerto USB y 1 puerto VGA.

- Se deben incluir 4 cables DAC SFP28 a SFP 28 para enlazar a 25GbE todos los puertos del nodo al switch Mellanox SN2010 existente en el CPD provincial de Jaén. Dichos cables DAC podrán ser activos o pasivos y deberán cubrir, al menos, una distancia de 3 metros.

Las características específicas mínimas de los nodos se describen en la siguiente tabla:

ID de Clúster	Nodos mínimos a incorp. al cluster	Características por nodo								
		CPU		RAM	Almacenamiento					
		Cores por Socket	Puntuación "Average CPU Mark"	Cantidad Total (GB)	Discos tier caliente			Discos tier frío		
					Tamaño			Tamaño		
					Unid.	TB	Tecnología	Unid.	TB	Tecnología
C1	1	12	20.000	512	2	3,84	SSD	8	4	HDD

4. GARANTÍA Y SOPORTE

El periodo de garantía será de 5 años para todos y cada uno de los elementos suministrados, incluyendo el software, y permitirá al SAS no solo el acceso al soporte ante incidencias software y al diagnóstico, suministro y sustitución de hardware, sino que también permitirá el acceso a actualizaciones de software, incluyendo nuevas versiones que se publiquen de los mismos, y *"firmware"* de los productos durante la vigencia especificada.

En cualquier caso, el soporte deberá contar con una cobertura de atención 24x7x365 y ser prestado por el fabricante del software, no se aceptarán propuestas en las que el soporte, ya sea parcial o totalmente, sea prestado por un tercero.

Los Acuerdos de niveles de servicio (ANS) para la atención por parte del soporte según la criticidad de las incidencias deberán ser:

- Prioridad 1 - Emergencia:
  - Definición: El sistema no está disponible.
  - Tiempo de respuesta máximo: 1 hora
- Prioridad 2 - Críticas:
  - Definición: El sistema está disponible, pero presenta problemas que tienen impacto en el servicio.
  - Tiempo de respuesta máximo: 4 horas
- Prioridad 3 - Normal:
  - Definición: Degradación del funcionamiento o rendimiento del sistema sin impacto en el servicio.
  - Tiempo de respuesta máximo: 8 horas
- Prioridad 4 - Consultas:
  - Descripción: consultas.
  - Tiempo de respuesta máximo: 24 horas

La asistencia in-situ para las incidencias de elementos hardware averiados o defectuosos deberá hacerse como máximo el siguiente día laborable al que se haya detectado el origen de la incidencia.

Por motivos de privacidad de los datos que sobre la plataforma se desplegarán, los discos averiados no serán devueltos al fabricante, quedando una vez reemplazados los mismos en propiedad del SAS.

Se facilitará por escrito la forma de abrir una nueva incidencia. En caso de haber varias formas de contacto en función del tipo de incidencia, se detallará dónde comunicar cada tipo de incidencia. Se podrá comunicar incidencias o consultar el estado de las que estén en curso por vía telefónica.

5. CONDICIONES ESPECÍFICAS

5.1. Horario del servicio de garantía y asistencia técnica multicanal

Las tareas necesarias para la ejecución del contrato, deberán ser realizadas en horario habitual de la FPS, que es el siguiente:

- De lunes a viernes, de 8:00h a 18:00h.

Es responsabilidad de la empresa adjudicataria y de sus delegados/as impartir todas las órdenes, criterios de realización del trabajo y directrices a sus trabajadores/as, siendo la FPS de todo ajena a estas relaciones laborales, y absteniéndose, en todo caso, de incidir en las mismas. Corresponde asimismo a la empresa contratista, de forma exclusiva, la vigilancia del horario de trabajo de los trabajadores, las posibles licencias horarias o permisos o cualquiera otra manifestación de las facultades del empleador. No obstante, es responsabilidad exclusiva del adjudicatario, en la forma establecida en los pliegos, asegurar que el servicio quede convenientemente cubierto.

5.2. Medios técnicos y materiales

La persona adjudicataria realizará los trabajos relacionados con la gestión de la garantía de los productos adquiridos con medios materiales propios (líneas de comunicaciones, equipos informáticos, teléfonos móviles, etc.).

5.3. Gastos de transporte

Todos los gastos de transporte y seguros que conlleve el suministro en los locales designados por el SAS serán por cuenta de la persona adjudicataria.

5.4. Inventariado, etiquetado y grabado de los bienes suministrados

Todos los bienes suministrados mediante el presente expediente requieren ser etiquetados para su inventariado por parte de la Junta de Andalucía, de cara a cumplir con lo dispuesto en la Ley 4/86, de 5 de mayo, del Patrimonio de la Comunidad Autónoma de Andalucía en su artículo 14, así como la Orden de 23 de octubre de 2012 por la que se desarrollan determinados aspectos de la política informática de la Junta de Andalucía.

El etiquetado se realizará mediante etiquetas que proporcionará la Junta de Andalucía; no obstante, hay que destacar que el proceso completo de etiquetado debe realizarlo la persona suministradora, y los costes asociados a este proceso estarán incluidos dentro de los trabajos a realizar dentro de esta contratación.

Por otro lado, los activos hardware objeto del contrato vendrán grabados con estampado en superficies directamente visibles, con medios indelebles, en base a la normativa vigente. No se admite grabado con tinta ni el grabado sobre placa fijada posteriormente por cualquier sistema al equipo. La persona adjudicataria debe adoptar el procedimiento que mejor se adapte en función del tipo de superficie (plástica o metálica) donde se vaya a realizar el grabado.

La persona adjudicataria deberá realizar todos los pasos indicados en el procedimiento de inventariado de bienes vigente en la Junta de Andalucía, y tomar todas las medidas necesarias para garantizar que los bienes son entregados con la correspondiente entrada en el Censo de Recursos Informáticos de la Junta de

Andalucía (CRIJA) y con la correspondiente etiqueta en los términos que describe el procedimiento de inventariado.

Es responsabilidad de la persona adjudicataria proporcionar la información de inventario necesaria para el correcto seguimiento de los activos del SAS, ya sea en su fase de provisión o de garantía. Igualmente, la persona adjudicataria se comprometerá al uso de la herramienta de gestión de activos del SAS, adecuándose a los métodos y tecnologías de recogida de información definidas por el SAS.

El soporte de dicha información será especificado por el SAS para todos los activos y sus elementos, tanto hardware como software. Asimismo, la persona adjudicataria deberá mantener actualizado dicho inventario por los mismos medios frente a los cambios debidos a sustituciones o recambios ocasionados por deficiencias detectadas con posterioridad a la entrega.

6. CONDICIONES GENERALES

Este apartado describe las condiciones generales para expedientes de contratación TIC. La aplicación concreta de cada una de ellas al objeto de esta contratación depende directamente del entorno tecnológico en el que se encuadra.

Definición de entorno tecnológico.

Las condiciones generales que son de aplicación directa en conexión con el entorno tecnológico descrito a lo largo del presente documento son las siguientes:

1. Seguridad	2. Tratamiento de datos de carácter personal	3. Propiedad intelectual del resultado de los trabajos
4. Interoperabilidad	5. Rediseño funcional y simplificación de procedimientos administrativos	6. Definición de procedimientos administrativos por medios electrónicos
7. Uso de certificados y firma electrónica	8. Práctica de la verificación de documentos firmados electrónicamente	9. Gestión de usuarios y control de accesos
10. Disponibilidad pública del software	11. Uso de infraestructuras TIC y herramientas corporativas.	12. Conformidad con los marcos metodológicos de desarrollo de software de la Junta de Andalucía
13. Desarrollo web: accesibilidad	14. Desarrollo web: páginas web orgánicas del SAS y puntos de acceso electrónico permitidos en la administración andaluza	15. Desarrollo web corporativa e intranet: apertura de Datos
16. Desarrollo web corporativa e intranet: apertura de Servicios	17. Cláusula sobre normalización de fuentes y registros administrativos Carpeta ciudadana	18. Carpeta ciudadana

6.1. Seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

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 aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes y las dimensiones de información relevantes, considerando las categorías de seguridad en las que recaen los sistemas de información objeto de la contratación según los criterios establecidos en el anexo I del ENS.

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.

La persona adjudicataria deberá tener en cuenta lo dispuesto en la Resolución de 8 de abril de 2021, de la Dirección Gerencia del Servicio Andaluz de Salud, por la que se aprueba la Política de Seguridad de las Tecnologías de la información y la comunicación (TIC) del Servicio Andaluz de Salud, así como las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía y la Unidad de Seguridad TIC del Servicio Andaluz de Salud.

Además, 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/).

Para todas las tareas de montaje, instalación y puesta en marcha que estén relacionadas con la integración/interoperabilidad de sistemas de información, ciberseguridad, conectividad a la red telemática y/o cualquier otra actuación relacionada con las TIC, se deberán seguir las indicaciones del equipo TIC del centro, así como la unidad de Seguridad TIC.

La persona adjudicataria deberá colaborar con el SAS en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o los interesados, y si corresponde, (iii) colaborar en la realización de evaluaciones de impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes, teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga. Para ello, comunicará previamente los datos de contacto en el ámbito TIC del responsable del sistema y el responsable de seguridad, y si procede, delegado de protección de datos.

Asimismo, pondrá a disposición del SAS, a requerimiento de éste, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en el contrato y colaborará en la realización de auditorías e inspecciones llevadas a cabo, en su caso, por el SAS.

Respecto a la cadena de subcontrataciones con terceros, en su caso, la persona adjudicataria principal lo pondrá en conocimiento previo del SAS para recabar su autorización y estarán sujetos a las mismas obligaciones impuestas para esta en materia de seguridad, confidencialidad y protección de datos.

En el contrato se debe establecer los procedimientos de coordinación en caso de incidentes de seguridad o de continuidad (desastres).

La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el ENS.

6.2. Tratamiento de datos de carácter personal

De acuerdo con lo establecido en el artículo 32 del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) en adelante RGPD, la figura del responsable del tratamiento, que recae en el Director Gerente del Servicio Andaluz de Salud (en adelante SAS), representado por cada Dirección Gerencia de los centros, realizará la evaluación de riesgos que determinen las medidas apropiadas para garantizar la seguridad de la información y los derechos de las personas usuarias. Asimismo, y como se detalla en el punto 2, el encargado del tratamiento, representado por la persona contratista, también evaluará los posibles riesgos derivados del tratamiento, teniendo en cuenta los medios utilizados (tecnologías de acceso, recursos utilizados, etc.) y cualquier otra contingencia que pueda incidir en la seguridad. La determinación de las medidas de seguridad que deben ser aplicadas por la persona contratista podrá realizarse mediante la remisión de toda la información a la plataforma Confluence corporativa de la STIC, donde se albergan las medidas de seguridad de tratamiento de información de ámbito general o para escenarios de tratamiento o cesión de información específicos. Como mínimo, se incorporarán las medidas establecidas en Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, establecidas para los sistemas de categoría de nivel MEDIO.

El encargado del tratamiento, junto con el responsable del tratamiento, establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad según lo identificado en la Evaluación de Riesgos que, en su caso, incluirán, entre otros:

a) La anonimización y el cifrado de datos personales;
b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico;
d) Un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

El encargado del tratamiento asistirá al responsable del tratamiento para que éste pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del RGPD. Se incluirán las funcionalidades necesarias que permitan atender los derechos de los titulares de los datos: acceso, rectificación, supresión, oposición, portabilidad, limitación y decisiones automatizadas.

El encargado del tratamiento pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En caso de violación de la seguridad de los datos personales, el encargado del tratamiento notificará sin dilación indebida y en un plazo máximo de 24 horas al responsable del tratamiento, las violaciones de la seguridad de los datos personales de las que tenga conocimiento. La notificación de las violaciones de la seguridad de los datos se realizará obligatoriamente mediante correo electrónico a los buzones del Delegado de Protección de Datos (DPD) y a la Unidad de Seguridad TIC (USTIC), junto con una comunicación al Centro de Gestión de Servicios TIC (CGES) del SAS a través de sus canales.

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

1) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.
2) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
3) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
4) Procedimientos para informar a las partes interesadas, internas y externas.
5) Procedimientos para:
   a) Prevenir que se repita el incidente.
   b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
   c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en el Reglamento Europeo de Protección de Datos (RGPD), en lo que corresponda.

El encargado de tratamiento prestará especial atención a las medidas de protección categorizadas en el ENS relacionadas con la protección de las aplicaciones informáticas (código [mp.sw] en el ENS) y desarrollo de aplicaciones (código [mp.sw.1] en el ENS).

1) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de producción en el entorno de desarrollo.
2) Se usarán pautas de desarrollo documentadas en la plataforma CONFLUENCE de la STIC que:
   a) Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
   b) Trate específicamente los datos usados en desarrollo y pruebas.
   c) Permita la inspección del código fuente.
3) Los siguientes elementos serán parte integral del diseño del sistema:
   a) Los mecanismos de identificación y autenticación.
   b) Los mecanismos de protección de la información tratada.
4) La generación y tratamiento de pistas de auditoría. Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

<u>Aceptación y puesta en servicio (código [mp.sw.2] en el ENS):</u>

1) Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. Se verificará que:

a) Se cumplen los criterios de aceptación en materia de seguridad.
b) No se deteriora la seguridad de otros componentes del servicio.

2) Las pruebas se realizarán en un entorno aislado (pre-producción).
3) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
4) Se realizarán las siguientes inspecciones previas a la entrada en servicio:
   a) Análisis de vulnerabilidades.
   b) Pruebas de penetración.

Protección de servicios y aplicaciones web (código [mp.s.2] en el ENS):

Los sistemas dedicados a la publicación de información deberán estar protegidos frente a las amenazas que les son propias.

1) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información sin autenticación, en particular tomando medidas en los siguientes aspectos:
   a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
   b) Se prevendrán ataques de manipulación de direcciones de recursos de internet (más conocidos por el término URL por sus siglas en inglés).
   c) Se prevendrán ataques de manipulación de fragmentos de información que se almacenan en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en inglés como «cookies».
   d) Se prevendrán ataques del tipo inyección de código.
2) Se prevendrán intentos de escalado de privilegios conforme a lo estipulado en la plataforma Confluence de la STIC.
3) Se prevendrán ataques de «cross site scripting».
4) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cache».

Firma electrónica [mp.info.4]

La firma electrónica es un mecanismo de prevención del repudio; es decir, previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada.

La firma electrónica garantiza la autenticidad del signatario y la integridad del contenido. Cuando se emplee firma electrónica solo se utilizarán medios de firma electrónica de los previstos en la legislación vigente.

1) Los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso:
   a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional
   b) Se emplearán, preferentemente, certificados reconocidos.
   c) Se emplearán, preferentemente, dispositivos seguros de firma.
2) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:
   a) Certificados.
   b) Datos de verificación y validación.
   c) Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.

d) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1) y 2).
e) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1) y 2).

Datos de carácter personal [mp.info.1]:

Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
Lo indicado en el párrafo anterior también se aplicará, cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información.

6.3. Propiedad intelectual del resultado de los trabajos

Todos los estudios y documentos, así como los productos y subproductos elaborados por la persona contratista como consecuencia de la ejecución del presente contrato serán propiedad de la Servicio Andaluz de Salud, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello la persona adjudicataria autor material de los trabajos. La persona adjudicataria renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato 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 del Servicio Andaluz de Salud, específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación, corresponden únicamente al Servicio Andaluz de Salud.

La presente cláusula no será de aplicación a los productos y herramientas preexistentes empleados para la ejecución del contrato protegidos por derechos industriales o de propiedad intelectual.

6.4. Interoperabilidad

Las ofertas garantizarán un adecuado nivel de interoperabilidad técnica, semántica y organizativa, conforme a las estipulaciones del Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI). En concreto, se cumplirán las Normas Técnicas de Interoperabilidad establecidas por dicho esquema. Se cuidarán especialmente los aspectos de interoperabilidad orientados a la ciudadanía, de tal forma que se evite la discriminación a los ciudadanos por razón de sus elecciones tecnológicas. El sistema implantará los protocolos ENIDOCWS y ENIEXPWS para que los documentos y expedientes electrónicos que se gestionen en el mismo puedan, a partir de sus códigos seguros de verificación, ser puestos a disposición e interoperar de manera estandarizada con otros sistemas y repositorios electrónicos de la Junta de Andalucía, así como remitirse a otras Administraciones si procede.

También se atenderá a los modelos de datos sectoriales relativos a materias sujetas a intercambio de información con la ciudadanía, otras Administraciones Públicas y entidades, publicados en el Centro de Interoperabilidad Semántica de la Administración (CISE) que resulten de aplicación.

Además, y en virtud del artículo 11.2 del RD 4/2010 por el que se establece el ENI, se hará uso de los siguientes formatos no incluidos en el catálogo de estándares del ENI para dar cobertura, en caso de que aplique, a funcionalidades y aplicaciones de ámbito sanitario:

- ISO/HL7 27931 – HL7 v2.x – FHIR DSTU2 – FHIR STU3
- ISO 12052 – DICOM, para el caso de imagen electrónica

La aplicación que se desarrolle/provea deberá integrarse con los sistemas de información corporativos siguiendo las pautas, normas y procedimientos definidos por la Oficina Técnica de Interoperabilidad del SAS, que actuará de asesor y coordinador de los diferentes circuitos a definir para que se pueda verificar la corrección de los flujos de información, accesibles a través de la página correspondiente del portal Confluence del SAS:

https://ws001.sspa.juntadeandalucia.es/confluence/collector/pages.action?key=INTERPUB

Este portal recoge toda la regulación en cuanto a normas y procedimientos de trabajo que ha identificado la STIC como imprescindibles para el aseguramiento de la calidad de los servicios de intercambio de información prestado a sus clientes, así como de calidad de la semántica corporativa necesaria para mantener la coherencia de los procesos.

Se cuidarán especialmente los aspectos de interoperabilidad orientados a la ciudadanía, de tal forma que se evite la discriminación a los ciudadanos por razón de sus elecciones tecnológicas. También se atenderá a los modelos de datos sectoriales relativos a materias sujetas a intercambio de información con la ciudadanía, otras Administraciones Públicas y entidades, publicados en el Centro de Interoperabilidad Semántica de la Administración (CISE) que resulten de aplicación.

Para la práctica de la verificación, mediante un código generado electrónicamente, de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, para el contraste de su autenticidad y la comprobación de su integridad, en el marco de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. y su normativa de desarrollo, y el apartado VIII (Acceso a documentos electrónicos) de la Norma Técnica de Interoperabilidad de Documento Electrónico, se utilizará la Herramienta Centralizada de Verificación, de acuerdo con el protocolo técnico disponible en el apartado correspondiente de la web de soporte de administración electrónica de la Junta de Andalucía.

6.5. Rediseño funcional y simplificación de procedimientos administrativos

Con carácter general se deberá tener en consideración que la aplicación de medios electrónicos a la gestión de los procedimientos, será precedida de la realización de un análisis de rediseño funcional y simplificación, de acuerdo con lo dispuesto en la Ley 39/2015, en el marco del principio general simplificación administrativa establecido en la Ley, y de la promoción de la aplicación del principio de simplificación en la presentación de escritos y documentos y en la tramitación de los expedientes que se realicen a través de redes abiertas de telecomunicación, de acuerdo con el artículo 5.4 del Decreto 183/2003, de 24 de junio, por el que se regula la información y atención al ciudadano y la tramitación de procedimientos administrativos por medios electrónicos (Internet).

Para ello se considerará el Manual de Simplificación Administrativa y Agilización de Trámites de la Administración de la Junta de Andalucía, aprobado por Orden de 22 de febrero de 2010 (BOJA núm. 52 de 17 de marzo) disponible en la siguiente dirección:

https://ws024.juntadeandalucia.es/ae/extra/manualdesimplificacion

6.6. Definición de procedimientos administrativos por medios electrónicos

La definición de los procedimientos deberá realizarse conforme a los conceptos y términos expresados en el documento Dominio Semántico del Proyecto w@ndA (ISBN 84-688-7845-6) disponible en la web de soporte de administración electrónica de la Junta de Andalucía. La citada web está accesible en la siguiente dirección:

http://www.juntadeandalucia.es/haciendayadministracionpublica/ae

6.7. Uso de certificados y firma electrónica

Para la identificación y firma electrónica mediante certificados electrónicos se atenderán las guías y directrices indicadas en el apartado correspondiente a la plataforma @firma en la web de soporte de administración electrónica de la Junta de Andalucía, en particular en lo relativo a la no utilización de servicios y componentes obsoletos, de custodia de documentos en la plataforma o cuya desaparición esté prevista para futuras versiones, a formatos de firma electrónica y la realización de firmas electrónicas diferenciadas y verificables para cada documento, realizándose en su caso las oportunas actuaciones de adecuación de las funcionalidades actualmente existentes en los sistemas incorporados en el objeto de la contratación. La citada web está accesible en la siguiente dirección:

http://www.juntadeandalucia.es/haciendayadministracionpublica/ae

Se utilizarán los servicios provistos por la implantación corporativa de la plataforma @firma gestionada por la Consejería competente en materia de administración electrónica.

6.8. Práctica de la verificación de documentos firmados electrónicamente

Para la práctica de la verificación, mediante un código generado electrónicamente, de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, para el contraste de su autenticidad y la comprobación de su integridad, en el marco del artículo 27.3.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el artículo 42.b) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y el apartado VIII (Acceso a documentos electrónicos) de la Norma Técnica de Interoperabilidad de Documento Electrónico, se utilizará la Herramienta Centralizada de Verificación, de acuerdo con el protocolo técnico disponible en el apartado correspondiente de la web de soporte de administración electrónica de la Junta de Andalucía.

6.9. Gestión de usuarios y control de accesos

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar, se tendrán en cuenta las estipulaciones que sobre seguridad hace la legislación vigente en materia de tratamiento de datos personales, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) así como de la legislación nacional vigente en materia de protección de datos, y el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En particular, se perseguirá:

- la correcta identificación de los usuarios (medida op.acc.1 del anexo II del ENS).
- la adecuada gestión de derechos de acceso (medida op.acc.4).
- la correcta selección e implantación de los mecanismos de autenticación (medida op.acc.5).

A. En relación con las directrices corporativas que se creen en materia de gestión de identidades.

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar (roles, gestión de login y password...) se deberán respetar las directrices que la Junta de Andalucía elabore en lo referente a la gestión de identidades y en su caso, adaptándose a la solución de single sign-on que la Junta haya provisto. Dichas Directrices se proporcionarán con la suficiente antelación, aportando la documentación técnica existente para tal fin.

B. En el caso de que en alguno de los sistemas, aplicaciones, herramientas, etc. objeto de contratación se gestionen trámites y actuaciones que se realizan con la Administración de la Junta de Andalucía por razón de la condición de empleado público.

El sistema deberá admitir, para los trámites y actuaciones que su personal realice con ella por razón de su condición de empleado público, el sistema de identificación de la plataforma de Gestión Unificada de Identidades de Andalucía (GUIA) de acuerdo con el artículo 25.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía

6.10. Disponibilidad pública del software

De conformidad con lo establecido en la orden de 21 de febrero de 2005, sobre disponibilidad pública de los programas informáticos de la administración de la Junta de Andalucía y de sus organismos autónomos, el sistema de información desarrollado pasará a formar parte del repositorio de software libre de la Junta de Andalucía, en las condiciones especificadas en la citada orden. La persona adjudicataria deberá entregar el código fuente del sistema de información desarrollado, así como la documentación asociada y la información adicional necesaria, en un formato directamente integrable en el repositorio de software libre de la Junta de Andalucía. De esta obligación quedarán exentos todos aquellos componentes, productos y herramientas que no habiéndose producido como consecuencia de la ejecución del contrato, estén protegidos por derechos de propiedad intelectual o industrial que no permitan la libre distribución o el acceso al código fuente.

La aplicación desarrollada será publicada en el repositorio de software libre de la Junta de Andalucía; viniendo acompañada además, junto con el software, de la documentación completa, en formato electrónico, referente tanto al análisis y descripción de la solución así como del correspondiente manual de usuario, con objeto de que este software pueda fácilmente ser usable.

6.11. Uso de infraestructuras TIC y herramientas corporativas.

En el marco de lo dispuesto sobre el impulso de los medios electrónicos en el art. 36.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía, se tendrán en cuenta todas las infraestructuras TIC (sistemas de información, tecnologías, frameworks, librerías software, etc.) que en la Junta de Andalucía tenga la consideración de corporativas u horizontales y sean susceptibles de su utilización. Se considerarán, entre otras, las siguientes:

- Para el modelado y tramitación de los flujos de trabajo ligados a procedimientos administrativos se deberá utilizar el tramitador TREW@ y herramientas asociadas (eximiéndose de esta obligación en el caso de flujos de trabajo que no estén ligados a procedimientos).
- @firma: la plataforma corporativa de autenticación y firma electrónica para los procedimientos administrativos, trámites y servicios de la Administración de la Junta de Andalucía.
- Autoridad de Sellado de Tiempo de la Junta de Andalucía.
- @ries: el registro unificado de entrada/salida.
- notific@: prestador de servicios de notificación.
- LDAP del correo corporativo para la identificación y autenticación de usuarios, hasta que se produzca la implantación definitiva del Directorio Corporativo de la Junta de Andalucía.
- port@firma: gestor de firma electrónica interna.
- Etc.

6.12. Conformidad con los marcos metodológicos de desarrollo de software de la Junta de Andalucía.

Durante la realización de los trabajos se tendrán en cuenta los recursos proporcionados por los marcos metodológicos vigentes de desarrollo de software en la Junta de Andalucía, así como las pautas y procedimientos definidos en éstos.

6.13. Desarrollo web: accesibilidad

Todos los sitios webs y aplicaciones para dispositivos móviles desarrollados o que sean mejorados de manera significativa en el marco del presente contrato deberán ser accesibles para sus personas usuarias y, en particular, para las personas mayores y personas con discapacidad, de modo que sus contenidos sean perceptibles, operables, comprensibles y robustos. La accesibilidad se tendrá presente de forma integral en el proceso de diseño, gestión, mantenimiento y actualización de contenidos de los sitios web y las aplicaciones para dispositivos móviles.

En este ámbito se deberán cumplir lo establecido por el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. En particular, se deberán cumplir los requisitos pertinentes de la norma UNE-EN 301-549:2019, de Requisitos de accesibilidad de productos y servicios TIC, o de las actualizaciones de dicha norma, así como de las normas armonizadas y especificaciones técnicas en la materia que se publiquen en el Diario Oficial de la Unión Europea y/o hayan sido adoptadas mediante actos de ejecución de la Comisión Europea.

Por último, como obliga la normativa se deberá realizar al menos una revisión anual de la accesibilidad de los sitios web y sistemas desarrollados o mejorados de manera significativa en el marco del contrato, así como actualizar y en su caso, elaborar, la correspondiente Declaración de accesibilidad de conformidad con el modelo europeo establecido Decisión de Ejecución (UE) 2018/1523 de la Comisión de 11 de octubre de 2018 por la que se establece un modelo de declaración de accesibilidad de conformidad con la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

6.14. Desarrollo web: páginas web orgánicas del SAS y puntos de acceso electrónico permitidos en la administración andaluza

El Decreto 622/2019 de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía, establece la tipificación de puntos de acceso electrónico permitidos en la administración andaluza. En este sentido, los trabajos de desarrollo que tengan relación con páginas webs orgánicas del SAS se adecuarán a los dispuesto en este Decreto y, por tanto, se llevarán a cabo las acciones oportunas para la integración de los contenidos de las páginas web orgánicas del SAS en el punto de acceso electrónico general, el portal de la Junta de Andalucía.

6.15. Desarrollo web corporativa e intranet: apertura de datos

El diseño y desarrollo informático deberá facilitar el acceso y descarga de todos los datos existentes en la aplicación, así como posibilitar su publicación en el Portal de Datos Abiertos de la Junta de Andalucía. Los datos se proporcionarán en formatos estructurados, abiertos e interoperables, de acuerdo con la normativa vigente de publicidad y reutilización de información pública

Los sistemas de información desarrollados deberán permitir la descarga de todos los datos en bruto y desagregados en varios formatos no propietarios estándar de facto como EXCEL (de las tablas que constituyan el núcleo de la aplicación, así como las tablas auxiliares para su interpretación) preferiblemente mediante API REST (interfaz de programación de aplicaciones), basado en estándares abiertos que permitirá el acceso automático a los datos y en tiempo real.
Si los anteriores conjuntos de datos contienen información de carácter personal, se realizarán la extracción de datos mediante un proceso de disociación o anonimización que garantice el cumplimiento de la Ley de Protección de Datos.

6.16. Desarrollo web corporativa e intranet: apertura de servicios

El diseño y desarrollo informático deberá estar orientado a la estrategia "API First", teniéndose en cuenta la necesidad de definir y publicar servicios comunes que puedan ser consumidos desde varios canales, sistemas u organismos. Este enfoque está basado en definir en la fase inicial una API de servicios externos e internos de la organización o sistema, para que los distintos interlocutores y canales puedan utilizar los servicios de la API en cuanto se publique.

La especificación OpenAPI (OAS) define un estándar para la descripción de APIs REST, que permite tanto a humanos como a servicios de integración descubrir y entender las capacidades y características de un servicio sin necesidad de acceder a los detalles de implementación del código fuente, documentación técnica, o detalles del tráfico de mensajes. Los servicios definidos apropiadamente a partir del estándar OpenAPI, permiten que un consumidor pueda entender e interactuar con un servicio remoto a partir de una implementación mínima.

En concreto, la definición de los servicios de la API se realizará cumpliendo las especificaciones OpenAPI establecidas por dicha organización (OAS). En relación a los estándares a emplear en el marco del presente contrato, las ofertas deben garantizar el cumplimiento y utilización del estándar y normas establecidas por OpenAPI, en los casos que fuese necesario.

6.17. Cláusula sobre normalización de fuentes y registros administrativos

Con la finalidad de asegurar la compatibilidad e interoperabilidad con otras fuentes y registros administrativos, el tratamiento de variables demográficas (sexo, edad, país de nacimiento, nacionalidad, estado civil, composición del hogar), geográficas (país, región y provincia, municipio y entidad de población, dirección, coordenadas) o socioeconómicas (situación laboral, situación profesional, ocupación, sector de actividad en el empleo, nivel más alto de estudios terminado) que se haga en el sistema seguirá las reglas para la normalización en la codificación de variables publicadas por el Instituto de Estadística y Cartografía de Andalucía accesibles a través de la URL:

http://www.juntadeandalucia.es/institutodeestadisticaycartografia/ieagen/sea/normalizacion/ManNormalizacion.pdf

6.18. Carpeta ciudadana

El sistema deberá integrarse con la Carpeta Ciudadana para informar a la ciudadanía sobre el estado de tramitación de sus expedientes administrativos y, en su caso, el acceso a su contenido, de acuerdo con el art. 38.2 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía y atendiendo al contrato del servicio Carpeta Ciudadana disponible en la web de soporte de administración electrónica de la Junta de Andalucía.

7. HERRAMIENTAS A EMPLEAR

La persona adjudicataria se compromete a usar las herramientas de gestión que indique la STIC. El uso de otras herramientas de gestión distintas a las indicadas por propia iniciativa de la persona adjudicataria no lo exime de esta obligación, siendo de su cuenta la dotación de los medios técnicos necesarios para su integración.

A continuación, se definen las herramientas que se usarán para la gestión de todos los servicios definidos, sin menoscabo de incorporación o sustitución de alguna de ellas por indicación expresa de la STIC durante la vigencia del contrato. La persona adjudicataria se compromete al uso de dichas herramientas según las instrucciones que se detallan a continuación.

1. Normativa TIC	2. Servicios de integración con las herramientas de gestión TIC	3. NWT: Nueva Web Técnica
4. JIRA y Confluence	5. MTI-SSHH	6. Herramienta CASE
7. Repositorio de código fuente	8. Repositorio de componentes	9. Catálogos para el desarrollo software
10. Sistema de integración continua	11. Sistema de gestión de la calidad del código fuente	12. Sistema de Gestión de la Configuración (CMS)
13. DMSAS	14. Symantec Endpoint Protection y Altiris Client Management Suite	15. Herramientas de gestión logística TIC
16. JARVIS	17. Aplican todas las anteriores	

7.1. Compendio de la normativa TIC

En el espacio NormativaTIC se enlazan todas las normas técnicas de la STIC. La persona adjudicataria se comprometerá a prestar los servicios contratados de acuerdo con este compendio normativo

https://ws001.sspa.juntadeandalucia.es/confluence/display/normativaTIC

Cualquier excepción al cumplimiento de esta cláusula deberá ser aprobada de forma previa al comienzo de las tareas por el SAS.

7.2. Servicios de integración con las herramientas de gestión TIC

Para optimizar los esfuerzos de gestión relacionados con las solicitudes que se registran y resuelven a través de las herramientas de gestión TIC, la persona adjudicataria debe dotarse de los medios técnicos necesarios para hacer uso de los servicios de integración provistos por la STIC y mantener actualizadas dichas integraciones en todo momento. Estas actualizaciones pueden ser motivadas por la evolución o incorporación de nuevos servicios de integración.

El detalle de estos servicios de integración, sus actualizaciones y procedimientos, se encuentran disponibles en:

https://ws001.sspa.juntadeandalucia.es/confluence/display/SERVCGESP/API+REST+Servicios+CGES

7.3. NWT: Nueva Web Técnica

Es la herramienta del SAS destinada a la gestión de solicitudes, incidencias, peticiones, problemas y configuración, los cuales se registrarán en este sistema informático, y se utilizarán como prueba documental para valorar el grado de cumplimiento del contrato.

La persona adjudicataria deberá conectarse a este sistema para la recepción de todos los avisos de solicitudes, corriendo por cuenta de la persona adjudicataria la dotación de los medios técnicos necesarios para su integración en el citado sistema.

El registro de incidencias y sus datos son confidenciales. La persona adjudicataria no divulgará su contenido a terceros sin la aprobación expresa del SAS.

El detalle del manual de la puede consultarse en

https://ws001.sspa.juntadeandalucia.es/confluence/pages/viewpage.action?pageId=26935915

7.4. JIRA y Confluence

Son las herramientas del SAS destinadas a la gestión del ciclo de vida del software, proyectos y conocimiento, y encargadas de la gestión y coordinación de los contratos de servicios para el mantenimiento de aplicaciones a medida, proyectos y conocimiento.

La persona adjudicataria deberá conectarse a estos sistemas para la recepción y gestión de todas las solicitudes de servicio relacionadas con el objeto del contrato, corriendo por cuenta de la persona adjudicataria la dotación de los medios técnicos, y licenciamiento en caso de ser necesario, para su acceso, uso e integración en los citados sistemas.

7.5. MTI-SSHH

Es la herramienta del SAS que representa la única fuente de información válida para el análisis de datos y para el cálculo de los ANS del contrato, así como para la comprobación de su cumplimiento.

Los ANS estarán disponibles y habrá un periodo en el que se actualicen en función de los datos que arrojen las herramientas operacionales que son fuentes para su cálculo. Llegado el día 10 del mes siguiente al del periodo de prestación del servicio, salvo que la STIC estime otra cosa, se cerrarán los procesos de cálculo de los ANS.

7.6. Herramienta CASE

Es la herramienta del SAS encargada de registrar de forma estructurada toda la información correspondiente a cada uno de los productos y proyectos de desarrollo de software, procurando así una visión completa de los mismos y modelando su comportamiento tanto a nivel tecnológico como de negocio, lo cual permite a su vez mantener traza con las fases de testing y control de calidad.

La persona adjudicataria deberá entregar en cada fase del ciclo de vida del software la versión correspondiente del producto en fichero nativo o importable en la herramienta CASE del SAS, según la información especificada en el espacio de NormativaTIC arriba mencionado.

7.7. Repositorio de código fuente

Es la herramienta del SAS destinada al almacenamiento del código fuente de los productos software desarrollados por el SAS.

La persona adjudicataria deberá conectarse a este sistema para la entrega del código fuente de productos software desarrollados en el ámbito de esta contratación, según el procedimiento definido para ello en el espacio de NormativaTIC arriba mencionado.

7.8. Repositorio de componentes

Es la herramienta del SAS destinada al almacenamiento y puesta a disposición de los distintos proveedores de software, tanto de las librerías necesarias para el desarrollo de los aplicativos, como de las librerías generadas por las diferentes aplicaciones desarrolladas.

La persona adjudicataria deberá conectarse a este sistema para la descarga de las librerías necesarias para los desarrollos realizados en el ámbito de esta contratación.

7.9. Catálogos para el desarrollo software

Existen tres catálogos principales que deben ser incluidos en todos los análisis que impliquen nuevas funcionalidades y/o modificaciones de productos software, con objeto de garantizar la coherencia interna de los datos y su alineamiento con la semántica de la organización.

- Catálogo de servicios de interoperabilidad: catálogo de servicios de interoperabilidad disponibles, ya sea a través de la plataforma SOA corporativa o directamente en las aplicaciones proveedoras.
- Catálogo de tablas maestras: catálogo de tablas que mantienen los datos maestros del SAS.
- Catálogo de componentes: catálogo de módulos y componentes disponibles para su reutilización en las distintas aplicaciones.

7.10. Sistema de integración continua

Es la herramienta del SAS destinada a la construcción automatizada del software a partir del código fuente entregado en el repositorio de código del SAS. La STIC será la responsable de la configuración de las tareas de construcción y empaquetado de cada entregable, según la información proporcionada a tal efecto por la persona adjudicataria.

La persona adjudicataria, por su parte, será el responsable de proporcionar las instrucciones y todos aquellos recursos software necesarios para la construcción y empaquetado de los entregables a partir de su código

fuente. La construcción del ejecutable a partir del código fuente deberá poder realizarse únicamente en base a lo dispuesto por el SAS para sus entornos y tecnologías de desarrollo, así como en los elementos disponibles en los catálogos antes mencionados.

Previamente a cualquier entrega, la persona adjudicataria deberá verificar la correcta construcción y empaquetado del software, únicamente, a partir de los recursos disponibles a través del repositorio de componentes corporativo, siendo responsabilidad exclusivamente suya los retrasos derivados de los defectos detectados durante dicho proceso en las instalaciones del SAS.

7.11. Sistema de gestión de la calidad del código fuente

Es la herramienta del SAS destinada a la revisión de la calidad del código fuente entregado en el repositorio de código fuente del SAS.

El equipo de la Oficina de Calidad del SAS será el responsable de la medición de los indicadores y de la configuración de las tareas revisión de la calidad del código fuente proporcionado con cada entregable.

La persona adjudicataria, por su parte, será el responsable de asegurar el cumplimiento de los mínimos de calidad definidos para el código fuente proporcionado con cada entregable en el repositorio de código del SAS. Previamente a cualquier entrega, la persona adjudicataria deberá verificar la calidad del código fuente entregado según los mínimos exigibles por la Oficina de Calidad, siendo responsabilidad exclusivamente suya los retrasos derivados de los defectos detectados durante el proceso de revisión de la calidad del código fuente en las instalaciones del SAS.

7.12. Sistema de Gestión de la Configuración (CMS)

CMS es la herramienta de destinada a controlar y gestionar los componentes y activos TIC. El CMS mantiene las relaciones entre los componentes del servicio y cualquier incidencia, problema, error conocido, cambio y documentación asociada. Actualmente el CMS aglutina la información de varias fuentes distintas o CMS físicas, que accesibles mediante un único interfaz, constituyen una CMS integral y federada.

7.13. DMSAS

DMSAS es el directorio activo del SAS, que constituye la única fuente de identificación y autenticación normalizada de la organización.

7.14. Symantec Endpoint Protection y Altiris Client Management Suite

El SAS enrolará a la persona adjudicataria en los actuales procedimientos de resolución remota, entre los que cabe destacar, sin ser exhaustivos:

- Gestión de inventario, de la configuración y de activos.
- Administración y despliegue de software.
- Ejecución de las políticas de actualización de parches establecidas.
- Gestión y despliegue de imágenes y maquetas definidas para cualquier elemento de la configuración.
- Control remoto de los equipos de puesto de trabajo digital.
- Ejecución de las políticas de protección y eliminación de virus informáticos.

Para ello, la persona adjudicataria deberá usar las herramientas corporativas del SAS: Symantec Endpoint Protection (SEP) y Altiris, para las cuales su personal estará convenientemente capacitado.

7.15. Herramientas de gestión logística TIC

El SAS dispone de diversas herramientas que dan cobertura a distintos aspectos de la gestión logística TIC y a las cuales la persona adjudicataria deberá integrarse para dar cobertura a todo el proceso: SIGLO (herramienta corporativa de gestión logística), SIGMA-MANSIS (gestión de activos), NWT (gestión de operación TIC), CMS (gestión de activos TIC), JIRA/Confluence (gestión de proyectos TIC), APOLO (gestión de almacenes TIC).

7.16. JARVIS

JARVIS es una aplicación realizada a medida para la recogida de peticiones de modificación y extracciones de datos desde Nueva Web Técnica y su lanzamiento automatizado y validado por la STIC a través de MS Orchestrator, alojando los resultados en un FTP corporativo al cual tienen acceso los resolutores de la petición.

De esta manera se agilizan las peticiones de lanzamiento (PL) de datos, se establece una trazabilidad concreta al respecto y se controlan las actuaciones en producción de los proveedores, incorporando adicionalmente una gestión de roles y permisos para cada uno de los actores involucrados

Adicionalmente, a través del uso de plantillas y variables para las actuaciones, se asegura la flexibilidad y adaptabilidad a las necesidades demandadas, mejorando los tiempos de resolución y la percepción del usuario final, al eliminar elementos de gestión innecesarios.

8. DEFINICIONES, ABREVIATURAS Y ACRÓNIMOS

En el presente Pliego de Prescripciones Técnicas serán de aplicación las siguientes definiciones:

- **AHV**: se refiere por sus siglas en inglés a Acropolis Hypervisor. Acrópolis es el hipervisor nativo que usa Nutanix para la implementación y ejecución de máquinas virtuales sobre los nodos de los clústeres hiperconvergentes.
- **AOS**: Sistema Operativo Acrópolis, por sus siglas en inglés.
- Clúster: conjunto de dos o más equipos o nodos, idénticos, que proporcionan la misma funcionalidad.
- **GPU**: unidad de proceso gráfico por sus siglas en inglés. Se trata de una unidad de procesador formado por muchos núcleos más pequeños y especializados para el procesamiento gráfico.
- **vGPU**: GPU virtual (graphics processing unit virtual, en inglés)
- **HCI**: Infraestructura Hiperconvergente por sus siglas en inglés. HCI es un enfoque de arquitectura basada en software que proporciona recursos de almacenamiento, cómputo y redes, de forma transparente al hardware que se utilice, con grandes capacidades de escalado horizontal. Todo ello permite que las operaciones de gestión y control sobre la infraestructura y los servicios disponibles sean gestionadas desde un único panel de control.
- **MV**: máquina virtual por sus siglas en inglés.
- **SDDC**: Centro de Datos Definido por Software por sus siglas en inglés.
- **Spine-leaf**: es una arquitectura de red que consta de dos capas: la capa leaf y la capa spine. La capa spine está formada por switches que realizan el enrutamiento y funcionan como la columna vertebral de la red. La capa leaf implica un switch de acceso que se conecta a puntos finales como servidores, dispositivos de almacenamiento. En la arquitectura leaf-spine, cada switch de leaf está interconectado con cada switch de spine. Con este diseño, cualquier servidor puede comunicarse con cualquier otro servidor con no más de una ruta de switch de interconexión entre dos switches de leaf.