ANEXO XIII

DECLARACIÓN DE APLICABILIDAD A LOS PRODUCTOS QUE LLEVEN INCORPORADOS PROGRAMAS INFORMÁTICOS, PARA LOS PROGRAMAS INFORMÁTICOS QUE CONSTITUYAN PRODUCTOS POR SÍ MISMOS O CUALQUIER PRODUCTO QUE SE CONECTE A LAS REDES DE LOS CENTROS SANITARIOS.

TITULO: SERVICIO DE DISPONIBILIDAD TECNOLÓGICA DEL SISTEMA DE PLANIFICACIÓN DOSIMÉTRICA, PRODUCTO SANITARIO, PARA TRATAMIENTO A PACIENTES MEDIANTE RADIOTERAPIA EXTERNA Y QUE OPERAN LOS SERVICIOS DE RADIOFÍSICA Y ONCOLOGÍA RADIOTERÁPICA DEL SERVICIO ANDALUZ DE SALUD

EXPEDIENTE: CC. 5101/2025 (Nº SIGLO 0000935/2025)

LOTE: [ ]Lote1 [ ]Lote2 [ ]Lote3

D./Dª. ……, con DNI. Núm , actuando:
☐ en nombre propio
☐ en representación de la entidad licitadora ……., con CIF núm.……
…,

DECLARA BAJO SU RESPONSABILIDAD

La veracidad de los datos incluidos en las tablas siguientes,

Que cuenta con certificado de conformidad en el ENS, para categorías MEDIA o ALTA, o en su caso, la declaración de conformidad para categoría BÁSICA para los servicios contratados incluyendo en su alcance, como mínimo, el ámbito objeto de la contratación. (marcar lo que proceda)	
Declaración de Conformidad para sistemas de categoría BÁSICA	
Certificación de conformidad para sistemas de categoría MEDIA	

Certificación de conformidad para sistemas de categoría ALTA	
Que está en proceso de obtención de la certificación de conformidad en el ENS	

Marcar lo que proceda a continuación:
Si: En el caso de que El adjudicatario afirme cumplir con la medida
No: En el caso de que El adjudicatario considere que no cumple con la medida
No aplica: En el caso de que El adjudicatario considere que la medida no le aplica
Propone Alternativa: En el caso de que El adjudicatario no cumpla con la medida y proponga medidas compensatorias igualmente efectivas.

Medidas de Seguridad	**Si**	**No**	**No aplica**	**Propone Alternativa**
POLÍTICA DE GESTIÓN DE VULNERABILIDADES				
Cláusula 1: Proceso de Identificación y Gestión de Vulnerabilidades				
Que ha implementado un proceso continuo y proactivo para la identificación y gestión de vulnerabilidades.				
El proceso se mantiene a lo largo del ciclo de vida de todos sus productos.				
El proceso incluye la consulta regular a bases de datos públicas de vulnerabilidades reconocidas internacionalmente.				
El proceso incluye el uso de fuentes de inteligencia de amenazas como informes de ciberseguridad y bases de datos de vulnerabilidades.				
Cláusula 2: Análisis Regular de Vulnerabilidades				
Que realiza análisis de vulnerabilidades periódicos en los dispositivos médicos objeto del contrato.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Se utilizan herramientas avanzadas de escaneo y pruebas de penetración.				
Los análisis pueden ser realizados en las instalaciones del adjudicatario, del fabricante del dispositivo, o cualquier otra ubicación adecuada.				
Los análisis pueden ser llevados a cabo directamente por El adjudicatario o por terceros autorizados.				
Que documenta exhaustivamente las vulnerabilidades conocidas y potenciales identificadas en cada dispositivo.				
Cláusula 3: Notificación y Plan de Corrección				
Que notificará debida y regularmente a el Servicio Andaluz de Salud los resultados de los análisis de vulnerabilidades llevados a cabo.				
Que propondrá planes de corrección y priorización de las debilidades en los dispositivos médicos destinado a ser aplicados sobre los dispositivos desplegados en las instalaciones del Servicio Andaluz de Salud.				
Cláusula 4: Implantación Inicial Libre de Vulnerabilidades				
Los dispositivos médicos adquiridos deberán ser implantados en los centros sanitarios libres de vulnerabilidades conocidas en el momento de la instalación.				
Si no es posible un despliegue inicial libre de vulnerabilidades conocidas, El adjudicatario proporciona al Servicio Andaluz de Salud el último informe de análisis de vulnerabilidades realizado, identificando las vulnerabilidades conocidas hasta la fecha y presentando un plan de corrección y priorización correspondiente.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Que especificará los mecanismos habilitados para la remediación continua de todas las vulnerabilidades no corregidas en el momento de la puesta en producción del dispositivo.				
AUDITORÍA Y REGISTRO DE ACTIVIDAD:				
Cláusula 5: Registros de Seguridad y Configuración de Logs				
Manifiesta que los sistemas de información asociados a los dispositivos médicos, así como, en su caso, los propios dispositivos médicos, permiten la activación y configuración de registros de seguridad.				
Declara que los sistemas y dispositivos son capaces de registrar eventos de seguridad importantes de manera detallada y continua.				
Expone que se mantienen logs detallados de todas las actividades de acceso a los dispositivos y sistemas, incluyendo accesos exitosos, intentos fallidos, cambios en la configuración, y cualquier otra actividad relevante.				
Expresa que la configuración de los dispositivos permite establecer políticas de retención de logs adecuadas para asegurar que los registros estén disponibles para auditoría durante un período determinado, de acuerdo con las mejores prácticas y regulaciones aplicables.				
Cláusula 6: Monitorización Continua y Revisión de Auditoría				
Indica que los dispositivos médicos y sus sistemas de información relacionados permiten la monitorización continua mediante sistemas automatizados desplegados por el Servicio Andaluz de Salud para la detección de intrusiones, accesos no autorizados, actividades sospechosas o no autorizadas.				
Manifiesta que los dispositivos médicos y sus sistemas de información relacionados disponen de la capacidad necesaria para que el Servicio Andaluz de Salud pueda llevar a cabo revisiones				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
periódicas de los registros de auditoría para identificar cualquier acceso no autorizado o actividad sospechosa.				
AUTENTICACIÓN Y AUTORIZACIÓN:				
Cláusula 7: Sistemas de Control de Acceso y Autenticación				
Manifiesta que los dispositivos médicos y sus sistemas de información relacionados disponen de un sistema de control de acceso robusto que garantiza que solo el personal autorizado pueda acceder a los datos personales de los pacientes.				
Declara que se establecen controles de acceso basados en roles que aseguran que solo el personal con las credenciales apropiadas pueda realizar acciones específicas dentro del sistema.				
Indica que se limita el acceso a funciones críticas según las responsabilidades de cada usuario.				
Cláusula 8: Procedimientos de Autorización de Acceso				
Establece que los mecanismos de control de acceso podrán alinearse con los procedimientos establecidos por el Servicio Andaluz de Salud para las autorizaciones de acceso a los dispositivos y sus sistemas de información relacionados.				
Expone que las políticas de acceso y autorización son revisadas y actualizadas periódicamente por El adjudicatario para reflejar cambios en los accesos de su personal y las necesidades de seguridad.				
Proclama que solo su personal necesario tiene acceso a información sensible.				
Indica que el Servicio Andaluz de Salud podrá llevar a cabo auditorías regulares para asegurar el cumplimiento de los				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
procedimientos de autorización de acceso y para identificar y corregir cualquier desviación.				
CONFIGURACIÓN SEGURA				
Cláusula 9: Configuración Inicial Segura				
Se garantiza que todos los dispositivos médicos son configurados inicialmente con una configuración segura, evitando el uso de configuraciones predeterminadas inseguras.				
Asegura que la configuración de seguridad inicial sigue las recomendaciones del fabricante del dispositivo y las mejores prácticas de la industria.				
Confirma que todas las credenciales predeterminadas son cambiadas inmediatamente después de la instalación del dispositivo y antes de su primer uso.				
Cláusula 10: Deshabilitación de Servicios y Configuración de Firewalls				
Deshabilita todos los servicios y puertos no necesarios en los dispositivos médicos para minimizar la superficie de ataque, asegurando que solo permanezcan funcionales los estrictamente necesarios para el funcionamiento del dispositivo.				
Garantiza que se suministrará la información necesaria para configurar firewalls con políticas de acceso estrictas para controlar el tráfico entrante y saliente, permitiendo exclusivamente las comunicaciones imprescindibles necesarias para el funcionamiento del dispositivo.				
Manifiesta que informará al Servicio Andaluz de Salud de las actualizaciones necesarias en las reglas de los firewalls para mantenerlos al día con las últimas firmas de amenazas y asegurar una protección continua.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Cláusula 11: Protección Física de los Dispositivos				
Para la instalación física de los dispositivos, la empresa sigue estrictamente las directrices del fabricante, garantizando que los componentes que actúan como servidores (como sistemas de gestión de bases de datos, servidores web o de aplicaciones) estén protegidos contra manipulaciones no autorizadas.				
Declara que estos componentes podrán estar ubicados exclusivamente en infraestructuras físicas que cumplen con las medidas de seguridad físicas establecidas por las políticas de seguridad del Servicio Andaluz de Salud.				
POLÍTICA DE ACTUALIZACIONES DEL SOFTWARE				
Cláusula 12: Políticas de Actualización				
Establece y mantiene políticas claras y documentadas para la actualización de hardware y software de los dispositivos médicos, garantizando que todos los dispositivos estén equipados con los últimos parches de seguridad y firmware antes de ser puestos en producción.				
Implementa un proceso regular y sistemático de actualización y parcheo para corregir vulnerabilidades de seguridad conocidas y mejorar la funcionalidad de los dispositivos.				
Cláusula 13: Actualizaciones Automáticas				
Siempre que sea factible y no represente un riesgo para el funcionamiento o el rendimiento del dispositivo, habilita procesos de actualización automáticos para aplicar parches de seguridad y mejoras.				
Garantiza que las actualizaciones automáticas son configurables para permitir el Servicio Andaluz de Salud definir horarios de actualización y así minimizar interrupciones en el servicio.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Cláusula 14: Mecanismos Seguros de Actualización				
Implementa mecanismos seguros para la actualización de software, asegurando la autenticidad e integridad de las actualizaciones.				
Dispone de un plan de actualización regular que incluye la aplicación de actualizaciones y parches.				
Cláusula 15: Evaluación de Impacto y Pruebas				
Lleva a cabo evaluaciones de impacto exhaustivas para evaluar el efecto de las actualizaciones en el funcionamiento del dispositivo y la seguridad del paciente antes de su implementación.				
Todos los parches y actualizaciones son revisados y probados en un entorno de pruebas antes de su aplicación en el entorno de producción, siguiendo procedimientos estandarizados para minimizar los riesgos de interrupciones.				
Cláusula 16: Documentación y Notificación				
Mantiene una documentación detallada para el seguimiento y registro de todas las actualizaciones aplicadas, incluyendo la fecha, el contenido de las actualizaciones y los dispositivos afectados.				
Notifica e informa a los usuarios y al personal relevante del Servicio Andaluz de Salud sobre las actualizaciones realizadas y cualquier cambio esperado en el funcionamiento del dispositivo.				
MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS				
Cláusula 17: Medidas de Seguridad para la Protección de Datos				
Manifiesta que los dispositivos médicos y sus sistemas de información relacionados, objeto de este contrato, aseguran el cumplimiento con las regulaciones de protección de datos como Reglamento (UE) 2016/679 RGPD y Ley 3/2018 LOPDGDD que				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
protegen la privacidad de los datos del paciente y la confidencialidad de los datos sensibles.				
Declara que en aquellos casos necesarios debido a la sensibilidad de la información tratada o en sistemas categorizados en categoría ALTA de acuerdo con el ANEXO I "Categorías de seguridad de los sistemas de información" del Esquema Nacional de Seguridad, los dispositivos tienen la capacidad para el cifrado de datos en tránsito y en reposo.				
Expone que los dispositivos utilizan mecanismos de cifrado fuertes para proteger los datos tanto en tránsito como en reposo, asegurando la confidencialidad de la información.				
POLITICA DE AUDITORÍA Y PRUEBAS DE SEGURIDAD				
Cláusula 18: Requisitos de Pruebas de Seguridad				
Acepta que el Servicio Andaluz de Salud establece los requisitos mínimos de pruebas de seguridad para todos los productos adquiridos, basándose en el umbral de riesgo aceptable definido por la organización.				
Consiente que el Servicio Andaluz de Salud puede realizar pruebas de penetración y auditorías periódicas de seguridad para validar la configuración segura y el rendimiento de los dispositivos antes de su despliegue en producción.				
Se podrá requerir el establecimiento de un entorno de pruebas que refleje el entorno de producción, permitiendo una evaluación precisa y detallada de los dispositivos médicos.				
Cláusula 19: Capacidad para Pruebas de Seguridad y Auditorías				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Manifiesta que los dispositivos médicos adquiridos tienen la capacidad de ser sometidos a pruebas de seguridad y auditorías que verifiquen al menos los siguientes aspectos:				
☒ Auditorías de seguridad sobre el registro de actividades de los dispositivos médicos y los sistemas de información relacionados.				
☒ Revisiones de auditoría para identificar accesos no autorizados o actividades sospechosas, incluyendo la monitorización en tiempo real mediante herramientas automatizadas y el envío de telemetría a herramientas de correlación de datos.				
☒ Revisión y evaluación del cumplimiento y la efectividad de las políticas de seguridad del Servicio Andaluz de Salud, incluyendo la necesidad de ajustes según sea necesario.				
☒ Revisión y evaluación del cumplimiento normativo para asegurar el cumplimiento con normativas y estándares relevantes.				
☒ Evaluación de los controles técnicos y los procedimientos de seguridad del proveedor.				
Establece que las auditorías y pruebas de seguridad, incluidas pruebas de penetración, podrán ser llevadas a cabo por el Servicio Andaluz de Salud de manera periódica, después de cambios significativos en los dispositivos o sus sistemas de información, o ante la sospecha de incidentes de seguridad.				
El Servicio Andaluz de Salud puede contratar a auditores externos para realizar evaluaciones independientes de la seguridad de los dispositivos médicos (Auditorías de Terceros).				
Cláusula 20: Pruebas de Validación Post-Despliegue				
Expone que el Servicio Andaluz de Salud podrá llevar a cabo pruebas de validación post-despliegue o pruebas de aceptación para confirmar que los dispositivos funcionan según lo esperado y cumplen con los requisitos de seguridad establecidos.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Llevará a cabo las tareas necesarias para corregir las vulnerabilidades detectadas antes de poner en producción los dispositivos.				
POLITICA PARA LICITACIONES QUE UTILIZAN SERVICIOS EN LA NUBE				
Cláusula 21: Cumplimiento Regulatorio				
Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información cumplen con el Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD), así como los requisitos de auditoría de pruebas de penetración, transparencia, cifrado, gestión de claves y jurisdicción de los datos.				
Se garantiza la conformidad con las normativas específicas para servicios en la nube, incluyendo las guías CCN-TIC correspondientes para SaaS, PaaS e IaaS.				
Cláusula 22: Cumplimiento con Guías CCN-TIC				
En función del modelo de servicio en la nube proporcionado, El adjudicatario cumple con lo establecido en la guía CCN-TIC correspondiente (SaaS, PaaS o IaaS).				
Cláusula 23: Localización y Ubicación Geográfica de los Datos Personales				
Informa al Servicio Andaluz de Salud sobre la ubicación geográfica de los datos, incluidas copias de seguridad y almacenamiento de logs, antes y durante el desarrollo del servicio.				
Si los dispositivos médicos o sus sistemas relacionados manejan datos personales ubicados en la nube, se asegura en todo momento que la localización de los servidores donde se almacenan estos datos está en Europa y se notifica cualquier cambio respecto a dicha localización.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Se cumple con la Ley 3/2018 LOPDGDD y demás normativa relacionada en materia de protección de datos.				
Cosiente que colaborará con el responsable del tratamiento en garantizar el ejercicio garantizará el ejercicio de los derechos de protección de datos conforme a las normativas aplicables				
Cláusula 24: Devolución y Destrucción de Datos				
Dispone de mecanismos que regulan la devolución de la información en el formato de datos y los plazos especificados, o en su defecto, la destrucción de los mismos, proporcionando evidencias certificadas de la realización.				
Establece un protocolo estandarizado para la devolución y destrucción de datos que incluye pasos detallados y verificables.				
Cláusula 25: Política de Respaldo y Recuperación				
Establece mecanismos para una política de respaldo y pruebas de recuperación que incluye:				
Identificación del alcance de los respaldos.				
Política de copias de seguridad.				
Medidas de cifrado de información en respaldo.				
Procedimiento de solicitud de restauraciones de respaldo.				
Realización de pruebas de restauración.				
Traslado de copias de seguridad (si aplica).				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Cláusula 26: Plan de Recuperación ante Contingencias				
Para garantizar la continuidad de los servicios, dispone y presenta un plan de recuperación ante contingencias que incluye:				
☒ Identificación y descripción de medios alternativos para la provisión de servicios.				
☒ Realización de al menos una prueba de recuperación anual con un informe detallado.				
☒ Actualización de la documentación del plan de recuperación según sea necesario.				
Cláusula 27: Transferencia de Conocimiento e Información al Finalizar el Contrato				
Al finalizar el contrato, desarrolla las acciones precisas para la transferencia de conocimiento e información, incluyendo la devolución de toda la información en el formato y plazo especificados, utilizando medios seguros.				
Establece un período de transición definido y planificado para asegurar una transferencia de conocimiento sin interrupciones.				
Cláusula 28: Planificación de la Restitución y Transferencia Tecnológica				
Presenta una planificación detallada para la restitución y transferencia tecnológica, contemplando medios, acciones de contingencia y riesgos potenciales.				
Cuando sea necesario, se incluye un período de transición para la gestión organizada del proceso de transferencia.				
Documenta un plan detallado de transición que incluye todas las etapas del proceso de transferencia, asegurando la coordinación efectiva entre todas las partes involucradas.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
POLITICA DE ACCESO REMOTO SEGURO PARA SERVICIOS DE MANTENIMIENTO Y RESOLUCIÓN DE INCIDENCIAS				
Cláusula 29: Autorización Previa para Herramientas de Acceso Remoto				
Solicitará autorización previa y expresa por parte del Servicio Andaluz de Salud para la instalación de cualquier herramienta de acceso remoto destinada a la prestación de servicios de mantenimiento y resolución de incidencias en dispositivos médicos y sus sistemas de información relacionados.				
Cláusula 30: Uso de Servicios VPN				
Para el acceso remoto a los dispositivos médicos y la prestación de servicios de mantenimiento y resolución de incidencias, se utilizan preferentemente los servicios corporativos de VPN sede a sede proporcionados por el Servicio Andaluz de Salud.				
Todas las comunicaciones realizadas a través de esta VPN están cifradas y autenticadas adecuadamente.				
Cláusula 31: Autenticación Multifactor				
Es obligatorio el uso de autenticación multifactor (MFA) para todos los accesos remotos a los dispositivos médicos y sus sistemas de información relacionados.				
Se implementan mecanismos avanzados de autenticación multifactor (MFA) para verificar la identidad de los usuarios que acceden al dispositivo.				
Cláusula 32: Autorización de Usuarios				
Sólo los usuarios previamente autorizados por el Servicio Andaluz de Salud a propuesta del adjudicatario tienen los derechos de				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
acceso necesarios para la prestación de servicios de mantenimiento y resolución de incidencias mediante acceso remoto.				
Cláusula 33: Propuesta de Herramientas de Acceso Remoto por el Adjudicatario				
Por razones operativas, el adjudicatario propone utilizar herramientas específicas para el acceso remoto a los dispositivos y sus sistemas de información relacionados para la prestación de servicios de mantenimiento y resolución de incidencias.				
Las herramientas propuestas respetan la arquitectura de seguridad del Servicio Andaluz de Salud, incluyendo la arquitectura de protección de perímetro tipo 6 (APP-6) según la Guía de Seguridad TIC CCN-TIC 811.				
Cláusula 34: Evaluación Excepcional de Herramientas de Acceso Remoto				
El adjudicatario puede demostrar el cumplimiento de las condiciones de seguridad necesarias de la herramienta propuesta para el acceso remoto mediante análisis y pruebas de seguridad realizadas por terceros independientes acreditados.				
Las herramientas propuestas por el adjudicatario no cuentan en ningún caso con vulnerabilidades conocidas.				
COMUNICACIÓN Y RESPUESTA A INCIDENTES				
Cláusula 35: Proceso Integral de Gestión de Incidentes				
Dispone de un proceso integral para hacer frente a los incidentes ocurridos en sus propias instalaciones que puedan tener impacto en la seguridad de los sistemas o servicios que presta el Servicio Andaluz de Salud.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Este proceso incluye procedimientos claros y detallados para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad.				
Se asignan roles y responsabilidades específicas a miembros del equipo de seguridad del adjudicatario para garantizar una gestión eficaz de los incidentes, incluyendo la capacidad de asignar recursos para investigar las causas, analizar las consecuencias y resolver el incidente.				
Cláusula 36: Procedimientos de Contención y Recuperación				
Implementa procedimientos de contención rápidos para limitar el alcance y el impacto de los incidentes de seguridad ocurridos en sus propias instalaciones que puedan afectar los sistemas o servicios que presta al Servicio Andaluz de Salud.				
Se incorporan estrategias para erradicar las amenazas y recuperar el funcionamiento normal de los dispositivos y servicios afectados lo más rápido posible.				
Cláusula 37: Notificación de Incidentes				
Notifica sin dilación a las partes interesadas y a las autoridades competentes sobre los incidentes de seguridad ocurridos en sus propias instalaciones, según lo requieran las normativas aplicables.				
Cuando el incidente pudiera afectar a los servicios prestados por el adjudicatario al Servicio Andaluz de Salud o este pudiera repercutir de alguna forma en sus infraestructuras tecnológicas, informará de las actuaciones llevadas a cabo para la resolución del incidente a los responsables de la información, responsables de los servicios afectados, al CERT de referencia, así como al responsable de los sistemas de información, el responsable de seguridad y el delegado de protección de datos del Servicio Andaluz de Salud.				
Se definen claramente las cadenas de mando y las responsabilidades de comunicación durante un incidente para				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
asegurar una respuesta coordinada y eficiente entre el adjudicatario y el Servicio Andaluz de Salud.				
Cláusula 38: Canales de Comunicación para Incidentes				
Para una comunicación ágil de los incidentes, se pueden utilizar múltiples canales de comunicación, como correo electrónico, mensajería instantánea y reuniones informativas, para asegurar que la información llegue a todos los involucrados.				
El adjudicatario establece canales claros para el reporte y seguimiento de incidentes de seguridad mediante protocolos de comunicación definidos, asegurando que todas las partes interesadas sean informadas adecuadamente durante un incidente.				
Esto incluye la comunicación con el personal interno del Servicio Andaluz de Salud, otros proveedores, autoridades y pacientes, en su caso.				
PROTECCIÓN CONTRA CODIGO DAÑINO				
Cláusula 39: Uso de software antivirus y de Detección y Respuesta ante amenazas.				
Siempre que las especificaciones del fabricante del dispositivo y sus sistemas relacionados lo permitan, se utiliza software para la protección contra código dañino y otras amenazas que impidan el uso de los dispositivos por intrusos o agentes maliciosos.				
Tienen siempre preferencia los sistemas de protección contra código dañino propios del Servicio Andaluz de Salud, ya que sus alertas son monitorizadas y supervisadas por la propia entidad y/o sus CERT de referencia.				
En aquellos casos en que el fabricante del dispositivo imponga una determinada herramienta para la protección contra código dañino, el adjudicatario especifica quién o qué organismo o empresa y de				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
qué forma se monitorizan las alertas ocurridas en los dispositivos objeto de adjudicación.				
Manifiesta que los productos o servicios de seguridad propuestos por el fabricante figuran en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPTIC) del Centro Criptológico Nacional o bien tener certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, de acuerdo con el artículo 19 del ENS				
Especifica de qué forma se comunicarán estas alertas al CERT de referencia del Servicio Andaluz de Salud.				
En aquellos casos contemplados en la cláusula anterior, el tiempo de comunicación de alertas es siempre inmediato, es decir, en tiempo real.				
Especifica que si el sistema relacionado con el dispositivo presta un servicio web, este estará protegido frente a ataques de manipulación, inyección de código e inyección SQL al menos mediante validación y saneamiento de entradas, uso de funciones seguras, control de accesos y privilegios, filtros y escapes de caracteres especiales, manejo adecuado de errores, etc.				
SEGURIDAD EN LA CADENA DE INSTALACIÓN				
Cláusula 40: Evaluación de Terceros Proveedores relacionados con la adjudicación.				
Dispone de mecanismos y criterios de seguridad rigurosos para la evaluación y selección de sus propios proveedores que tengan relación con esta adjudicación. Estos criterios incluyen la revisión de las políticas de seguridad, prácticas de manejo de datos, y medidas de ciberseguridad implementadas por los proveedores.				
Cuenta con la capacidad para llevar a cabo auditorías periódicas de seguridad de sus proveedores para asegurar que cumplen con los requisitos de seguridad establecidos.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
Las auditorías incluyen evaluaciones de vulnerabilidades, revisiones de cumplimiento normativo y pruebas de penetración. En su defecto, se podrán exigir las certificaciones de seguridad equivalentes de acuerdo con la normativa aplicable.				
Cláusula 41: Contratos y Acuerdos				
El adjudicatario incluye cláusulas de seguridad específicas en todos los contratos y acuerdos con sus proveedores relacionados con esta adjudicación. Estas cláusulas cubren aspectos como la protección de datos, la respuesta a incidentes, la gestión de acceso y la obligación de mantener actualizadas las medidas de seguridad.				
Estos contratos se revisan periódicamente con sus proveedores para asegurar que las cláusulas de seguridad sigan siendo relevantes y efectivas. Las revisiones tienen en cuenta cambios en las normativas, avances tecnológicos y lecciones aprendidas de incidentes de seguridad pasados.				
CONCIENCIACIÓN Y FORMACIÓN EN SEGURIDAD				
Cláusula 42: Programas de Formación				
El adjudicatario cuenta con programas de formación en ciberseguridad para todos sus empleados. Esta formación cubre los fundamentos de la ciberseguridad, la protección de datos, el reconocimiento de amenazas comunes y las políticas de seguridad de la organización.				
Los programas ofrecen una formación continua y actualizaciones periódicas sobre nuevas amenazas y mejores prácticas de seguridad.				
Cláusula 43: Concienciación de Seguridad				
Mantiene campañas de concienciación regulares para mantener la seguridad cibernética en la mente de todo el personal.				

Medidas de Seguridad	Si	No	No aplica	Propone Alternativa
RESOLUCIÓN DE CONFLICTOS EN LA APLICACIÓN DE LAS CLAUSULAS DE SEGURIDAD				
Cláusula 44: Equilibrio Funcionalidad y Seguridad				
Entiende que la aplicación de alguna de las cláusulas de seguridad de este anexo puede afectar a la disponibilidad de los servicios que presta el dispositivo, pueda suponer un perjuicio para el rendimiento del mismo o se pueda poner en peligro la seguridad del paciente, y lo comunica al Servicio Andaluz de Salud de forma inmediata mediante esta declaración de aplicabilidad.				
Propone al Servicio Andaluz de Salud medidas compensatorias alternativas y acompaña su propuesta de la justificación adecuada, para que el Servicio Andaluz de Salud atienda las razones expuestas por El adjudicatario y evalúe la pertinencia o no de las excepciones propuestas.				
Declara que las medidas propuestas son equivalentes en seguridad a las medidas compensatorias alternativas propuestas y no suponen un incremento en el riesgo para la seguridad del Servicio Andaluz de Salud.				

(Lugar Fecha y firma)