ANEXO V PPT: CONDICIONES TIC.

CLÁUSULAS TIC PARA SISTEMAS DE INFORMACIÓN INCLUIDOS EN LA PROPUESTA

A continuación, se definen todos los requerimientos técnicos, de: equipamientos, sistemas y procesos, que debe cumplir cualquier tipo de sistema informático que venga incluido en la propuesta, bien sea solicitada directamente en la licitación, bien como sistema incluido dentro del conjunto del suministro a realizar o incluso en el caso de que sea una mejora ofertada por el operador económico que no haya sido solicitada por el licitante.

La Subdirección de Tecnologías de la Información y las Comunicaciones (en adelante, STIC) del SAS en base a la Resolución SA 0157/2013 de 4 de abril de la Consejería de Salud queda establecida como la encargada de la prestación de servicios TIC en los diferentes centros de titularidad de la Consejería de Salud, lo que le confiere el carácter de único órgano competente en materia TIC de dichas entidades.

En base a ello, serán de obligado cumplimiento las normativas y políticas de seguridad vigentes establecidas por la STIC, que estarán a disposición de los interesados y serán actualizadas con carácter periódico.

Todas las peticiones de instalación, puesta en marcha o incorporación de nuevos dispositivos, aplicaciones sanitarias o sistemas de información necesitan de la aprobación expresa y validación de su idoneidad por parte de la STIC provincial.

En concreto estas normativas afectan a todos los sistemas informáticos (en adelante “Elementos TIC”) incluidos en la propuesta, como, por ejemplo: servidores, PCs, impresoras, PDAs, dispositivos móviles, dispositivos médicos y sus accesorios considerados software y hardware, dispositivos de red, sistemas de información, sistemas empotrados, integraciones de sistemas existentes, etc. La anterior lista es orientativa y la aplicación de esta normativa no sólo se aplica a estos elementos sino a cualquier otro elemento TIC interno o externo que esté incluido en la oferta.

La Subdirección TIC del SAS adopta como marco de referencia la Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada como ITIL, que son buenas prácticas destinadas a facilitar la gestión del ciclo de vida de servicios de tecnologías de la información y comunicaciones.

Asimismo, tal como indica el Esquema Nacional de Seguridad (en adelante ENS), como parte de estas cláusulas se establecerán también unos Acuerdos de Niveles de Servicio mínimos que aseguren el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados.

Como parte de la implementación de estas medidas de seguridad se pueden realizar por parte de la Administración auditorías periódicas de seguridad de cualquiera de las partes del sistema, de cara a garantizar la correcta aplicación de dichas medidas e incluso a incrementar la prevención de posibles eventos adversos de seguridad o disponibilidad.

Por otra parte, además de las disposiciones indicadas en estas cláusulas, se incluyen de forma implícita todos los marcos legales actuales y futuros que sean de obligado cumplimiento para los sistemas de información de la Administración Pública.

1.1. Normativa general para el equipamiento TIC

En los siguientes apartados se detallan los aspectos relacionados con el equipamiento y accesorios a suministrar, y la normativa relacionada con las TIC que se obligatorio cumplir:

- Aspectos de equipamiento homologado a suministrar.
    - Descripción de las características mínimas de los equipos y sus periféricos y de sus condiciones de suministro.
- Normativas de seguridad aplicables a los sistemas.
    - Criterios de seguridad que deben cumplir los elementos.
- Normativas de interoperabilidad e integración.
    - Caso que los sistemas a implementar puedan disponer de interconexiones con sistemas ya implantados en el SAS, tanto para los sistemas de información corporativos, como para los locales y para los horizontales.

1.1.1. Acuerdos de nivel de servicio (ANS) de la garantía mínimos

Como medio para garantizar la calidad de la garantía y siguiendo las indicaciones del Esquema Nacional de Seguridad, se establecen los siguientes ANS mínimos, que se aplicarán en el periodo de garantía del equipo. Es compromiso por parte de la empresa adjudicataria cumplirlos.

Estos ANS podrán evolucionar a lo largo de la ejecución del contrato, y su periodo de garantía, con el fin de conseguir una mejora continua en la calidad del servicio efectivamente proporcionado. Los recursos, tanto humanos como de otra índole, disponibles para el servicio de garantía, deberán ser dimensionados de forma cualitativa y cuantitativa como mínimo para garantizar los ANS vigentes en cada momento.

Los ANS se basarán en la definición de unos indicadores de calidad que reflejen de forma objetiva la calidad del servicio real proporcionado, con especial atención a los aspectos más críticos del mismo, y en el establecimiento de un umbral o valor mínimo de calidad para cada uno de ellos. Se han elaborado atendiendo a los siguientes criterios:

- El establecimiento de indicadores de calidad del servicio de garantía prestado, de manera que el SAS pueda realizar una evaluación objetiva de los servicios y que la empresa adjudicataria de esta licitación tenga una base para la corrección de las eventuales deficiencias en la prestación y para la mejora de sus procesos y organización.

- La automatización del seguimiento y control de los indicadores de calidad del servicio de garantía recogidos en los ANS. Los datos para la revisión de los indicadores del ANS se obtendrán de las distintas herramientas ya implantadas en el SAS.

- La empresa adjudicataria se comprometerá a realizar todas las acciones organizativas necesarias para permitir un adecuado control de todos los ANS identificados como mínimos en este pliego.

El SAS, a través de su dirección técnica de centro, podrá proponer cambios en la estructura de los ANS mínimos requeridos, que en todo caso deberán ser consensuados con la empresa adjudicataria. Los cambios podrán afectar tanto a los elementos del servicio objeto de medición como a la frecuencia, la unidad de medición y el nivel de servicio.

1.1.1.1. Condiciones de medida

En el cálculo de los indicadores no se contabilizarán los tiempos que se indican a continuación:

- No contabilizarán como tiempo de indisponibilidad las paradas programadas que se realicen en las condiciones preestablecidas y acordadas.

- No se contabilizarán las demoras que estén completa y exclusivamente en el ámbito de las responsabilidades de terceros (otros proveedores externos, personal ajeno al servicio, el propio SAS, etc.).

- Pérdidas de servicio debidas a causa de fuerza mayor (incendios, inundaciones, etc.), aunque en este caso se aplicarán los acuerdos alcanzados en el proceso de continuidad.

3.1.1.2 Indicadores

El seguimiento de los niveles de servicio se realizará en base a indicadores. El concepto de incidencia, prioridad en la clasificación de incidencias, intervención, tiempo de respuesta, etc., y los procesos que guían su gestión, se encuentran definidos en UNIFICA, el portal de normas técnicas del SAS.

INDICADOR	DEFINICIÓN	UNIDAD	OBJETIVO
	Porcentaje de incidencias con tiempo de resolución en plazo Según la tipología, impacto y urgencia de la incidencia, se establece una prioridad a la misma. Se calcularán los siguientes indicadores, según la prioridad asignada, del total de incidencias con tiempo de resolución en plazo entre todas las incidencias resueltas por el proveedor para la misma prioridad.		
IO_01	• **Porcentaje de incidencias con tiempo de resolución en plazo, con prioridad muy alta:** el tiempo máximo de resolución de la incidencia será de 4 horas hábiles de servicio desde la asignación de la incidencia.	Porcentaje	IO_01 >= 90%
IO_02	• **Porcentaje de incidencias con tiempo de resolución en plazo, con prioridad alta:** el tiempo máximo de resolución de la incidencia será de 12 horas hábiles de servicio desde la asignación de la incidencia.	Porcentaje	IO_02 >= 80%
IO_03	• **Porcentaje de incidencias con tiempo de resolución en plazo, con prioridad normal:** el tiempo máximo de resolución de la incidencia será de 18 horas hábiles de servicio desde la asignación de la incidencia.	Porcentaje	IO_03 >= 70%

INDICADOR	DEFINICIÓN	UNIDAD	OBJETIVO
	Tiempo medio de resolución de incidencias Según la tipología, impacto y urgencia de la incidencia, se establece una prioridad a la misma. Se calcularán los siguientes indicadores según la prioridad asignada, como la suma del tiempo de resolución de todas las incidencias entre todas las incidencias resueltas por el proveedor para la misma prioridad.		
IO_04	• **Tiempo medio de resolución de incidencias, con prioridad muy alta**	Horas hábiles	IO_04 <= 4
IO_05	• **Tiempo medio de resolución de incidencias, con prioridad alta**	Horas hábiles	IO_05 <= 12
IO_06	• **Tiempo medio de resolución de incidencias, con prioridad normal**	Horas hábiles	IO_06 <= 18
	Tiempo de sustitución de elemento hardware Para aquellas incidencias que requieran para su resolución definitiva de la sustitución de un elemento hardware, se establece el tiempo de sustitución de elemento hardware como el tiempo comprendido entre la asignación inicial de la incidencia y la sustitución completa del elemento hardware afectado.		
IO_07	• **Porcentaje de incidencias con tiempo de sustitución de elemento hardware en plazo.**	Porcentaje	IO_07 >= 80%
IO_08	• **Tiempo medio de sustitución de elemento hardware.**	Horas hábiles	IO_08 <= 24

IO_09	**Porcentaje de incidencias asignadas al adjudicatario con incumplimiento en el plazo de resolución que son reclamadas** Porcentaje de incidencias asignadas al adjudicatario que, con incumplimiento en el plazo de resolución según su prioridad, son reclamadas respecto del total de incidencias asignadas al adjudicatario.	Porcentaje	IO_09 <= 1%
INDICADOR	**DEFINICIÓN**	**UNIDAD**	**OBJETIVO**
IO_10	**Porcentaje de incidencias resueltas por el adjudicatario que son reabiertas** Porcentaje de incidencias resueltas por el adjudicatario que son reabiertas respecto del total de incidencias resueltas por el adjudicatario. Se entiende resuelta por el adjudicatario aquella incidencia en la que es el propio adjudicatario el que hace la propuesta de cierre de la incidencia.	Porcentaje	IO_10 <= 1%

1.1.2. Equipamiento homologado a suministrar

Todo el equipamiento informático que se suministre debe cumplir con estos criterios de homogenización mínimos, que van encaminados a que su funcionamiento dentro de los sistemas del SSPA sea lo más homogéneo posible y no genere ningún tipo de incompatibilidad, problemática colateral o coste adicional a la Administración Pública.

La relación entre el adjudicatario y la STIC debe iniciarse siempre desde la unidad de gestión o servicio de referencia destino del equipamiento.

Dicho interlocutor contactará con STIC por la vía establecida entre las partes, y siempre con una antelación mínima de al menos dos semanas a la instalación o conexión de equipos, indicando la empresa adjudicataria del contrato y estableciendo una primera reunión de inicio de proyecto donde la STIC solicitará toda la información necesaria para evaluar la propuesta.

La visita de técnicos o personal comercial de las empresas proveedoras, deberá ser convenientemente programada, el personal estará adecuadamente acreditado, y mostrará su acreditación a quien se la requiera, debiéndola llevar visible en sus desplazamientos por los centros.

1.1.2.1. Características generales que aplican a todos los elementos.

1.1.2.1.1. Suministro:

El material se deberá suministrar en las instalaciones del centro destinadas a su configuración y puesta en marcha.
La empresa adjudicataria deberá proporcionar todo el hardware y software necesario para la puesta en marcha del sistema ofertado, cumpliendo siempre con las características que indique la STIC, tanto para el sistema de producción como para la salvaguardia de las copias de seguridad de los datos.
El hardware ofertado deberá contar con mecanismos de tolerancia a fallos y alta disponibilidad que permitan el mantenimiento del servicio con las garantías necesarias para la finalidad del mismo.
No se aceptarán como válidas soluciones que cuenten con equipamiento ya existente en el SAS, salvo que así se diga expresamente en el Pliego de Prescripciones Técnicas.

1.1.2.1.2. Licencias:

La solución debe contemplar todas las licencias de software necesarias, propias o de terceros, para su puesta en marcha asegurándose el proveedor de cumplir con la normativa explícita de cada fabricante para los productos que incluyan.
Asimismo, en el caso de incluir licencias propietarias de uso limitado de alguno de los productos, deberán incluirse el número de ellas necesario para dar cobertura a todos los puestos de trabajo donde se use el sistema de información a implantar, y por todo el tiempo por el que tenga vigor el presente contrato.

1.1.2.1.3. Garantía:

Las garantías de reparación de todo el material TIC entregado deben cubrir el plazo completo del contrato, con un mínimo de 2 año, y debe garantizarse la disponibilidad de piezas de repuesto por un mínimo de 10 años adicionales. Dicha garantía debe cubrir piezas, mano de obra y cualquier otro tipo de coste de reparación de forma que el elemento suministrado pueda volver a quedar operativo en el menor plazo posible. Caso de no poder repararse, la empresa suministradora deberá sustituir el dispositivo por uno de características similares o superiores al averiado.

Durante la vigencia del presente contrato, y su garantía, la empresa adjudicataria será responsable del seguimiento del estado de los equipos, la coordinación, planificación y resolución de las averías y/o problemas que pudieran producirse, la definición de ventanas de intervención para el servicio de soporte, la verificación de resolución al cierre de la solicitud y el registro y validación de posibles actualizaciones en la base de datos de software o hardware del SAS.

1.1.2.1.4. Consumibles:

Todos los elementos proporcionados deben cumplir el criterio de que sus consumibles sean adquiribles a través del catálogo de productos del SAS, disponible en SIGLO.

En el caso de no estar el consumible necesario incluido en dicho catálogo, el proveedor será el responsable de gestionar su alta en el mismo antes de que sea necesario realizar la primera adquisición del consumible. En su defecto será el proveedor el responsable de suministrar el material necesario sin coste para el SAS hasta que se cumpla el punto anterior.

1.1.2.1.5. Compatibilidad ofimática:

Según la Instrucción N.º 4/2016 de la Viceconsejería, para la actualización de la ofimática corporativa de la Consejería de Salud, y la ley 11/2007 de 22 de Junio, de acceso electrónico e los ciudadanos a los Servicios Públicos, las aplicaciones deberán ser compatibles con la ofimática libre, no vinculadas obligatoriamente a Microsoft u otro proveedor propietario, y para el formato de documento: "*la única opción posible para el intercambio de documentos ofimáticos editables tales como hojas de cálculo, documentos de texto e imágenes y presentaciones, el siguiente formato: ISO/IEC 26300:2006 Information technology – Open Document Format for Office Applications (OpenDocument) OASIS 1.2 (ODF)*"

1.1.2.1.6. Gestión del ciclo de vida del sistema:

CGES es el organismo de gestión de peticiones de la STIC siendo webcges y/o NWT la herramienta destinada a la gestión de las solicitudes de servicio de operación (incidencias, peticiones y problemas). Cualquier petición relacionada con TIC deberá registrarse en este sistema informático, y se utilizará como prueba documental para valorar el grado de cumplimiento de los ANS establecidos, en caso de que los hubiera.

Por ello el adjudicatario está obligado a utilizar dicha gestión de peticiones en CGES, siendo este el principal canal desde donde los usuarios realizarán las distintas solicitudes de servicio y en el que se gestionará su resolución. Será siempre CGES la herramienta nativa para la gestión del servicio, independientemente de que la empresa internamente prefiera optar por otras soluciones propias de gestión que lleve en paralelo. El ciclo de vida de las peticiones se originará en CGES y la empresa adjudicataria será responsable de trabajar con dicha herramienta desde principio a fin de cada petición, siendo obligatorio el reporte y cierre de la petición en CGES. La STIC proporcionará al proveedor toda la documentación necesaria que debe aportar para su alta en el sistema o para su integración con una herramienta propia, o cualquier otro mecanismo autorizado expresamente por la STIC provincial.

1.1.2.1.7. Niveles de soporte:

Se establecen dos niveles de soporte que el proveedor deberá cubrir, en función de la criticidad del sistema contratado:

Los sistemas de criticidad normal o baja deben garantizar una atención al usuario en horario laboral de 8:00 AM a 8:00 PM, de forma que cualquier usuario del sistema pueda registrar una petición de asistencia a través de CGES, o cualquier otro mecanismo autorizado expresamente por la STIC provincial.

El soporte deberá incluir:

- Resolución de incidencias de usuarios.
- Atención de peticiones especiales relacionadas con la continuidad de servicio.
- Consultas de formación sobre la herramienta.
- Resolución de dudas sobre el uso del sistema.

El sistema de contacto para este soporte debe estar claramente identificado por el proveedor en la vía de contacto y los plazos de respuesta esperados.

La resolución de las incidencias de software clínico en ningún caso serán responsabilidad de la STIC. Las incidencias hardware tendrán soporte de la STIC según el acuerdo alcanzado entre las partes y siempre teniendo en cuenta la garantía de las máquinas y el correcto inventariado en la Base de Datos de Recursos Informáticos (DRI) en CGES.

En caso de conflicto sobre la responsabilidad entre varios resolventes o proveedores a la hora de tener que solucionar determinada incidencia o tarea, prevalecerá el criterio de la STIC motivando su decisión.

1.1.2.1.8. Conexión remota y acceso externo:

La constitución de la Red Corporativa de la Junta de Andalucía por la Consejería de Presidencia de la Junta de Andalucía establece que está terminantemente prohibido la instalación de cualquier tipo de línea de datos o conexión remota que no sea gestionada por dicha entidad, así que no están permitidas conexiones de datos de terceros de ningún tipo.

La única vía de conexión para proporcionar soporte remoto a los equipamientos TIC del SAS es mediante solicitud de VPN de la Red Corporativa de la Junta de Andalucía, bien personal para personas físicas concretas, bien en formato Sede a Sede. La STIC proporcionará los formularios necesarios que el proveedor debe rellenar para solicitar dicha conexión. Caso de que dicha conexión implique un coste, en ningún caso se podrá repercutir al SAS.

La única vía de conexión a PC del SAS es mediante el software de Control remoto instalado y configurado por la propia STIC. Dicha conexión será de carácter autentificada, aceptada expresamente por el usuario

y sujeta a todas las normas de Protección de Datos actuales y futuras que sean de cumplimiento. Está totalmente prohibido la desinstalación o desconfiguración de dicho software por parte del proveedor.

La conexión mediante otro tipo de herramientas como Escritorio Remoto, acceso directo a Bases de Datos, etc. será siempre bajo la aprobación, en cada caso, de la STIC de forma expresa, y requieren una validación explícita de las conexiones.

En caso de no poder proporcionarse el acceso remoto que solicita el adjudicatario, o que no sea posible llevar a cabo la conexión, será responsabilidad del proveedor enviar recursos in-situ para que resuelva el problema, no pudiendo convertirse esta imposibilidad de conexión en una razón para no resolver la incidencia y no dar el nivel de soporte necesario.

1.1.2.1.9. Gestión de identidad:

Toda herramienta que exija autenticación de usuarios y/o validación de perfiles de usuarios deberá implementar su conexión al directorio activo corporativo, DMSAS, y a la herramienta de Gestión de Identidad del SAS (Identic). La documentación necesaria para ello será aportada por la STIC, siendo obligación del proveedor hacer las modificaciones necesarias en sus sistemas para que se cumplan estas tres premisas:

- La autenticación de usuarios será siempre contra DMSAS.
- La gestión de perfiles estará integrada con Identic.
- La activación y desactivación de usuarios será gestionada por DMSAS.
- Integración se haga extensiva a la herramienta MACO, gestión de identidad de Diraya.

1.1.2.1.10. Documentación entregable:

Como parte de la solución y antes de finalizar el periodo de puesta en marcha, el proveedor deberá entregar como documentación adicional la siguiente información:

- Mapa de elementos físicos y lógicos instalados, con un inventario detallado de los elementos físicos y/o lógicos para proceder a darlos de alta, si procede, tanto en la DRI como en la CMDB (Nomenclatura ITIL) correspondiente.
- Mapa de integraciones.
- Elementos físicos y lógicos a monitorizar y la forma de realizar dicha tarea.
- Elementos de los que será necesario realizar copia de seguridad, su ubicación, la técnica necesaria para realizar la copia y su periodicidad. Incluyendo el procedimiento de cómo se podría proceder a la comprobación de que la copia de seguridad es válida y fiable.
- Documentación de las licencias instaladas y de las garantías de los equipos.

- Documentación de las posibles exclusividades para la contratación de los mantenimientos, que deberá ser visada como válida por la Unidad de Asesoría Jurídica.
- Teléfonos y/o correos de contacto para soporte y sus horarios.
- Importe anual de los mantenimientos de los sistemas instalados pasado el periodo de garantía, incluyendo las actualizaciones que resulten del equipo, tanto a nivel de software como de hardware, durante dicho periodo.

1.1.2.2. Criterios especiales por tipo de equipamiento:

Se diferencian los criterios en función del tipo de equipamiento: PC o estaciones de trabajo, Terminales ligeros, impresoras, electrónica de red, servidores y otros dispositivos de red**.**

1.1.2.2.1. Servidores y puntos de red:

Albergando las más de 400 aplicaciones departamentales que prestan servicio en la Provincia, la infraestructura a implantar debe ser muy modular y muy escalable. Si por cada una de estas aplicaciones se instalara un servidor básico los requerimientos de espacios en los Centros de Procesos de Datos (CPD) del SAS serían mayores a los disponibles, y por tanto no es posible autorizar implantaciones que dispongan de esta arquitectura.

Es por ello que la STIC tiene implantado un sistema de infraestructuras virtualizadas. Esto ofrece tanto reducción de la infraestructura física necesaria, como lo niveles de alta disponibilidad necesarios para un entorno crítico como el sanitario, pues se permite funcionar a la máquina virtual en varios servidores físicos. Todo ello redunda en una reducción de los costes de explotación y mantenimiento importantes.

Igualmente, la electrónica de red necesaria para integrarse con un 100% de garantías de interoperabilidad y correcto funcionamiento en las redes de los centros exige que la propia STIC tenga una lista de equipos recomendables de cara a montar infraestructura de red.

En los proyectos donde la instalación de nuevos puntos de red corresponda al adjudicatario, deberá este realizar la instalación de los mismos cumpliendo con los criterios de la STIC. Todos los requisitos en este aspecto son a modo de resumen:

- La instalación debe ser realizada por un proveedor certificado.
- El cableado debe ser UTP Categoría 6E o superior.
- El punto de red a instalar será doble (2 tomas en rosetas adyacentes).
- La ubicación donde irán los puntos de red nuevos será determinada por el personal de la STIC junto con el responsable de la Unidad destino.
- En función de la ocupación y el número de puntos necesario se puede solicitar al proveedor la inclusión de nuevos paneles de parcheo en el armario “Rack” destino, en consonancia a los ya existentes.

- Toda instalación de punto de red debe ir acompañada de sus dos latiguillos finales (equipo y parcheo) de las distancias necesarias
- La nomenclatura y timbrado de las rosetas será correlativa a las existentes en el armario destino y según las normas de la STIC.
- El punto debe certificarse según la categoría exigida y con la entrega de la documentación de dicha certificación se entregará también un plano de la ubicación de los nuevos puntos.
- Si el número de puntos así lo justifica, la STIC podrá solicitar al proveedor la adquisición de un número de *switches* de red proporcional al número de puntos a instalar.

- El punto de red no recibirá servicio mientras no se cumplan todos los requerimiento expuestos por la STIC.
- Está terminantemente prohibido la instalación de elementos de red intermedios (*hubs*, *microswitches*, duplicadores, etc.) que vayan destinados a "multiplicar" los puntos disponibles en una zona usando una única toma de red existente, al igual que la instalación de nuevos *Racks* de comunicaciones**.**

1.1.2.2.2. Otros dispositivos de red:

Cualquier otro dispositivo de red que se necesite conectar como parte del proyecto, deberá ser aprobado previamente por la STIC, que en caso de que sea necesario, consultará previamente con el Servicio Técnico del SAS correspondiente (bien sea de Electromedicina o de Mantenimiento)[1] del centro.

En los casos donde esté justificado, los dispositivos pueden ser conectados a redes privadas por la seguridad del resto de la red o de los propios dispositivos.

1.1.3. Normativa de seguridad, parcheado de sistemas y normalización de equipos cliente

1.1.3.1. Preámbulo:

A lo largo de los años la política de seguridad de infraestructuras TIC en el SAS se ha ido revisando y actualizando llegando a tener un parque de equipos cliente controlado y supervisado. Esto ha hecho que el número de incidentes adversos en temas de seguridad haya sido leve como consecuencia de esta situación.

Sin embargo, las nuevas técnicas de ataques utilizadas por los desarrolladores de amenazas y la gran interconexión que existe en la actualidad entre todos los sistemas pueden desembocar en graves crisis y pérdidas de datos de carácter sanitario debido a fallos de seguridad que podrían haber sido evitados.

[1] O la Subdirección a la que pertenezca en cada caso.

Como consecuencia de lo expuesto, es necesario que de forma URGENTE y PRIORITARIA se implementen de forma FORZOSA las políticas de seguridad vigentes (tanto en la firma del contrato como las futuras) a TODOS los equipos conectados en red dentro de centros del SAS.

En la mayoría de los casos de infecciones de virus masivas hoy en día en las instalaciones que se han visto afectadas, los problemas han sido provocados por equipos desactualizados o fuera del marco de seguridad de la empresa. Por ello es importante recalcar que esta normativa no sólo aplica a los equipos propiedad del SAS, sino que se debe hacer extensiva a todos los equipos conectados a la red, independientemente de la empresa que lo gestione. "Una cadena es tan débil como lo sea el más débil de sus eslabones".

Todos los puntos desarrollados en estas prescripciones están amparados por las normativas recogidas en los apartados siguientes

1.1.3.2. Normativa interna de seguridad

A modo de revisión y para poder tener un marco de referencia común se resumen aquí las políticas a implementar:

1. Todo equipo con sistema operativo Windows conectado a la red de datos del SAS debe estar integrado en el Dominio de Active Directory corporativo, conocido como DMSAS, su sistema operativo incluirá la licencia de Windows apropiada para poder hacer esta conexión.
2. Todos estos equipos serán parcheados de forma automática y obligatoria para aplicar todas las recomendaciones de actualizaciones críticas de seguridad del sistema operativo, liberados por el fabricante de este. También deberán permitir la inclusión del agente de monitorización e inventario que decida el SAS, actualmente Altiris.
3. Todos los equipos deben tener el antivirus corporativo instalado, configurado, actualizado y activo para el análisis de amenazas en tiempo real y actualizaciones automáticas periódicas. Igualmente, todos los equipos serán escaneados en busca de virus de forma periódica y continua y los ficheros infectados serán limpiados o en caso necesario e inevitable eliminados.
4. La nomenclatura de los equipos cumplirá obligatoriamente con el estándar SAS de nombrado de PC, servidores, electrónica y otros dispositivos de red e impresoras.
5. Los usuarios que trabajen en los equipos no tendrán en ningún caso permisos de administrador sobre este, ni capacidad de desactivar el antivirus o demás mecanismos de seguridad indicados con anterioridad.
6. Todo equipo que se detecte que incumple las normas anteriormente citadas, que se comporte de forma sospechosa o que sea fuente de amenazas, será desconectado y aislado de la red del SAS y deberá ser analizado y verificado su funcionamiento por parte del proveedor en un entorno controlado antes de volver a conectarse. El proveedor, y nunca el SAS, será el único responsable de las pérdidas de servicio y problemas que se generen como consecuencia de esta situación.

7. El acceso a los sistemas de información del SAS podrá ver deshabilitado temporalmente a cualquier usuario que voluntaria o involuntariamente actúe contra las normas indicadas. Dicho acceso sólo podrá reactivarse tras analizar el motivo de este comportamiento.
8. Toda empresa colaboradora con el SAS que disponga de equipos conectados a la red de este organismo está obligada a cumplir estas normas de forma obligatoria y sin excepciones. Cualquier problema que sea provocado por equipos que no cumplan estas normas será responsabilidad de dicha empresa.

1.1.3.3. Documento de "consentimiento informado":

Como en toda normativa, se pueden contemplar excepciones puntuales que será necesario analizar caso por caso y determinar, por parte de la STIC, si se permiten dichas excepciones o no.

Para poder proceder a evaluar dichos casos, será necesario que los responsables de las Unidades de Gestión, Servicios o Unidades Administrativas de los centros donde se encuentren o vayan a ser instalados los equipos, o en su caso el responsable legal de la empresa que solicite esta excepción remita a la Subdirección TIC de la provincia el documento de solicitud, cuya plantilla estará disponible en la Intranet del centro.

Las solicitudes serán evaluadas por la STIC, no siendo de aplicación hasta su aprobación y firma. No se podrá proceder a la instalación del sistema hasta que no se reciba confirmación del resultado.

1.1.4. Normativa de integraciones

En caso de que el sistema adquirido deba tener algún tipo de conectividad con los demás sistemas corporativos o locales, deberá cumplir las siguientes capacidades de integración:

- La solución aportada deberá cumplir las normas y procedimientos de Interoperabilidad de la STIC actuales y tener facilidad para adaptarse a las futuras que se vayan definiendo y publicando.

- Estas integraciones deberán estar certificadas por la OTI (Oficina Técnica de Interoperabilidad) en entornos de preproducción y verificadas funcionalmente por el personal técnico de la STIC antes de su puesta en producción. Todos los detalles del proceso de certificación se hallan en Unifica (https://ws001.juntadeandalucia.es/unifica/) y cualquier duda al respecto puede ser aclarada a través del correo interoperabilidad.oca.sspa@juntadeandalucia.es.

- Este proceso de certificación incluye de forma ineludible la presentación de un análisis previo de uso de la información en el que se definan el flujo de trabajo del circuito cubierto en formato estándar BPMN (Business Process Model and Notation), datos maestros a consumir, eventos que disparan los intercambios de información, etc. Una vez superado el proceso, la aplicación aparece como certificada en el Catálogo de Aplicaciones Certificas para el uso de Servicios de la STIC constando versión, centro y servicios certificados.

- No se autorizará el consumo de ninguna información a aplicaciones no certificadas en todos los extremos contemplados en el proceso.

1.1.4.1. Normativa de integraciones de imagen médica:

Las soluciones de imagen médica deberán poder integrarse con el RIS-PACS corporativo del SAS y/o con otros RIS-PACS en servicio en los Centros.

Las soluciones deberán ser compatibles con los siguientes servicios:

- Dicom 3.0
- DicomSend
- DicomPrint
- Dicom Storage
- DicomWorkList Management
- Dicom MPPS (Modality Performed Procedure Step)
- DicomQuery and Retrieve

El adjudicatario deberá aportar los documentos de conformidad DICOM del equipamiento o soluciones que incorpore al servicio de los centros.

1.2. Marco de referencia legal de dichas normativas

Resolución de 27 de septiembre de 2004 del Manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.

Donde se cita, por ejemplo, en el punto 5.8: “Los usuarios están obligados a cumplir las medidas de seguridad diseñadas por la Administración de la Junta de Andalucía, así como las prevenciones que al efecto se establezcan.”.

Decreto 1/2011 y Decreto 70/2017 sobre Política de seguridad de las tecnologías de la información y comunicaciones.

Artículo 6: “La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de la Administración de la Junta de Andalucía, siendo estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.”

ENS - El Real Decreto 3/2010, de 8 de enero, que determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. También conocido como "Esquema Nacional de Seguridad"[2].

En sus Capítulos II y III establece los principios básicos de seguridad y los requisitos mínimos que permitan la protección adecuada de la información. Los principios básicos establecen puntos de referencia para tomar decisiones. Los requisitos mínimos deben cumplirse siempre.

El cumplimiento del ENS se debe exigir también a los Sistemas de Información que estén operados por terceros local o remotamente – e, incluso, en las dependencias de los terceros. También se hace referencia explícita a sistemas que, aun no prestando directamente servicio al ciudadano, si debido a algún incidente de seguridad en esos sistemas se impidiera o perturbara la atención al mismo, como por ejemplo une equipamiento de radiología o una maquinaria de análisis y ayuda al diagnóstico.

El epígrafe 2.16 de las "Preguntas Frecuentes"[3] sobre el ENS, publicado por el Centro Criptológico Nacional, indica explícitamente que "Las medidas de seguridad que deben adoptar los proveedores de servicios en ningún caso las fijará el propio proveedor, sino que serán las determinadas por la Administración Contratante, en virtud de la naturaleza de los servicios prestados".

Asimismo, se establece la responsabilidad de suscribir el contrato de prestación del servicio incluyendo los Acuerdos de Nivel de Servicio a los que hubiera lugar.

También en su Artículo 9 especifica que: "Las medidas de seguridad se reevaluarán y actualizarán periódicamente".

RGPD - Reglamento General de Protección de Datos – Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea de 27 de abril de 2016 – DOCE 4.5.2016- L119 que entrará en vigor el 25 de mayo de 2018.

[2] https://administracionelectronica.gob.es/ctt/ens#.WhshQxNSxpg

[3] https://www.ccn-cert.cni.es/publico/dmpublidocuments/ENS-FAQ.pdf