REGISTRO DE LEVANTAMIENTO DE INFORMACIÓN:	
Código de Esquema:	THYS-GSI-201707
Versión de Esquema:	V-001
Fecha de elaboración:	12/7/2017

1.	**1.1 DENOMINACIÓN DEL PERFIL OCUPACIONAL.**	**GESTIÓN DE SISTEMAS INFORMÁTICOS**
	1.2 DENOMINACIÓN DEL ESQUEMA	**GESTIÓN DE SISTEMAS INFORMÁTICOS**
2.	**ALCANCE DE LA CERTIFICACIÓN.**	La certificación se hará con base al perfil completo; por todas las unidades de competencia.
	3.1 Descripción del/los trabajo/s.	**UC1 Administrar los dispositivos hardware del sistema.** 1.1. Elaborar y mantener inventarios de los componentes físicos del sistema para asegurar su localización y disponibilidad según las normas de la organización 1.2. Analizar y parametrizar los dispositivos hardware, monitorizando y evaluando su rendimiento para optimizar el funcionamiento del sistema y proponer, en su caso, modificaciones o mejoras según las necesidades funcionales existentes 1.3. Implementar y optimizar soluciones hardware de alta disponibilidad para garantizar y asegurar la protección y recuperación del sistema ante situaciones imprevistas según el plan de contingencias previsto 1.4. Planificar las ampliaciones y crecimiento del sistema proponiendo nuevas configuraciones para asumir incrementos futuros en la carga de trabajo o usuarios según las necesidades de explotación. 1.5. Definir las condiciones ambientales y de seguridad apropiadas para evitar interrupciones en la prestación de servicios del sistema según especificaciones del fabricante y el plan de seguridad de la organización. **UC2 Instalar, configurar y administrar el software de base y de aplicación del sistema.** 2.1. Instalar y configurar el sistema operativo de servidor para asegurar la funcionalidad del sistema según las necesidades de la organización. 2.2. Elaborar y mantener inventarios del software del sistema para garantizar su localización y disponibilidad según las normas de la organización. 2.3. Instalar y configurar aplicaciones corporativas para atender funcionalidades de usuarios según el plan de implantación de la organización 2.4. Elaborar el plan de soporte a los usuarios, coordinando al personal técnico de apoyo y mantenimiento para asegurar el uso de las funciones del sistema informático. 2.5. Configurar y administrar los recursos del sistema para optimizar el rendimiento según los parámetros de explotación de las aplicaciones. 2.6. Planificar la realización de copias de seguridad así como la recuperación de las mismas para mantener niveles adecuados de seguridad en los datos según las necesidades de uso y dentro de las directivas de la organización. 2.7. Auditar la utilización de recursos del sistema para asegurar un rendimiento óptimo según los parámetros del plan de explotación. **UC3 Asegurar equipos informáticos.** 3.1. Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad. 3.2. Configurar servidores para protegerlos de accesos no deseados según las necesidades de uso y dentro de las directivas de la organización. 3.3. Instalar y configurar cortafuegos en equipos y servidores para garantizar la seguridad ante los ataques externos según las necesidades de uso y dentro de las directivas de la organización.
		UC1 Administrar los dispositivos hardware del sistema. 1.1. Elaborar y mantener inventarios de los componentes físicos del sistema para asegurar su localización y disponibilidad según las normas de la organización 1.1.1. Identifica el hardware y los componentes físicos del sistema correctamente y enumeran exhaustivamente para conocer su disponibilidad actual. 1.1.2. Describe detalladamente el inventario hardware para informar de las características, configuración actual, situación exacta y estado de cada dispositivo según las normas de la organización. 1.1.3. Modifica las nuevas adquisiciones, cambios producidos en el hardware o en su configuración en el inventario para mantenerlo actualizado.

1.1.4. Detalla y referencia la documentación para la instalación del hardware en la documentación generada y se guardan convenientemente para su uso posterior
1.1.5. Interpreta correctamente la documentación técnica, tanto si está editada en castellano o en las lenguas oficiales de las comunidades autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector
1.2. Analizar y parametrizar los dispositivos hardware, monitorizando y evaluando su rendimiento para optimizar el funcionamiento del sistema y proponer, en su caso, modificaciones o mejoras según las necesidades funcionales existentes
1.2.1. Selecciona las técnicas o herramientas de monitorización a utilizar en función de las características del sistema para optimizar su funcionamiento.
1.2.2. Emplea las técnicas o herramientas de monitorización seleccionadas con destreza
1.2.3. Preparando el sistema para su monitorización, obteniéndose las estadísticas de rendimiento, programaciones de alertas y otros elementos de monitorización.
1.2.4. Establece los criterios de rendimiento del sistema según las disposiciones generales establecidas por el fabricante, y los particulares establecidos por la organización para obtener una monitorización adecuada.
1.2.5. Recoge y presenta los datos producidos de la monitorización de forma clara y concisa mediante la utilización de técnicas de representación.
1.2.6. Analiza la representación del rendimiento del sistema generada por la monitorización, para localizar posibles pérdidas o degradaciones de rendimiento y proponer las modificaciones necesarias.
1.2.7. Parametriza los dispositivos físicos para mejorar el rendimiento y corregir las anomalías de funcionamiento detectadas en el sistema.
1.3. Implementar y optimizar soluciones hardware de alta disponibilidad para garantizar y asegurar la protección y recuperación del sistema ante situaciones imprevistas según el plan de contingencias previsto
1.3.1. Resuelve las incidencias de instalación y configuración del hardware consultando la documentación técnica y los servicios de asistencia técnica.
1.3.2. Realiza la verificación de la instalación y configuración de los dispositivos físicos y sus controladores para el almacenamiento masivo y copias de seguridad, de modo que se pueda comprobar según los estándares y las normas de calidad y seguridad establecidas por la organización.
1.3.3.Efectúa la gestión de la reparación o sustitución de los componentes hardware averiados de acuerdo con las especificaciones técnicas del sistema y siguiendo el procedimiento de instalación establecido en la documentación técnica facilitada por el fabricante y los planes de implantación de la organización.
1.3.4. Realiza las verificaciones de los componentes sustituidos para asegurar su correcto funcionamiento según los estándares y las normas de calidad y seguridad establecidas por la organización.
1.3.5. Garantiza la integridad de la información y la continuidad en el funcionamiento del sistema durante la resolución de los problemas o desajustes, tomando las medidas preventivas de seguridad necesarias y activando los posibles procedimientos de explotación alternativos.
1.3.6. Restaura y actualiza la información original y copias de seguridad para que el sistema vuelva a entrar en explotación siguiendo el protocolo de seguridad establecido.
1.3.7. Supervisa el almacenamiento de las copias, comprobando que se cumplen los estándares de seguridad establecidos por la organización.
1.3.8. Implementa correctamente los servidores redundantes y otros sistemas de alta disponibilidad según especificaciones del fabricante y normas de la organización.
1.3.9. Interpreta correctamente la documentación técnica tanto si está editada en castellano o en las lenguas oficiales de las comunidades autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.
1.4. Planificar las ampliaciones y crecimiento del sistema proponiendo nuevas configuraciones para asumir incrementos futuros en la carga de trabajo o usuarios según las necesidades de explotación.
1.4.1. Analiza y valora el hardware para realizar informes de posibles necesidades futuras, así como la viabilidad de posibles mejoras y actualizaciones.
1.4.2. Analiza adecuadamente los informes de la organización acerca de futuros incrementos en la carga de trabajo o número de usuarios utilizando técnicas ajustadas a la situación.
1.4.3. Representa el sistema mediante herramientas matemáticas y de modelado analítico para analizar el rendimiento con las nuevas cargas añadidas.
1.4.4. Analiza los datos obtenidos a través del modelado y simulación del sistema para determinar si las nuevas cargas son asumibles.
1.4.5. Evalúa los dispositivos físicos disponibles en el mercado para proponer los más adecuados al sistema y que

		garanticen la absorción de la carga de trabajo planteada. 1.4.6. Planifica y ejecuta la implantación de nuevos dispositivos minimizando sus efectos sobre la explotación del sistema, optimizando los rendimientos del mismo y adecuando la tecnología según la evolución del mercado. 1.5. Definir las condiciones ambientales y de seguridad apropiadas para evitar interrupciones en la prestación de servicios del sistema según especificaciones del fabricante y el plan de seguridad de la organización. 1.5.1. Conoce e interpreta las especificaciones técnicas de los dispositivos y el plan general de seguridad de la organización adecuadamente para la adecuación del sistema. 1.5.2. Establece y contrasta los requerimientos ambientales y condiciones de alimentación eléctrica de los dispositivos físicos con las posibilidades de la instalación para evitar incidencias e interrupciones en el servicio. 1.5.3. Establece las condiciones de ergonomía, seguridad y aprovechamiento del espacio disponible para la correcta ubicación de los equipos y dispositivos físicos.
2.4. Realizar las operaciones de corte asignadas, empleando el sistema más adecuado y	**3.2 Descripción de las/s tarea/s.**	"UC2 Instalar, configurar y administrar el software de base y de aplicación del sistema. 2.1. Instalar y configurar el sistema operativo de servidor para asegurar la funcionalidad del sistema según las necesidades de la organización. 2.1.1. Instala el sistema operativo del servidor siguiendo los procedimientos y lo indicado en la documentación técnica. 2.1.2. Realiza la verificación de los componentes del sistema operativo y controladores de dispositivos mediante pruebas de arranque y parada, y la utilización de herramientas software de verificación y diagnóstico, de modo que se pueda comprobar que los componentes son reconocidos y habilitados y no aparecen conflictos según lo dispuesto por la organización. 2.1.3. Configura los parámetros del sistema operativo para garantizar la integridad y fiabilidad del sistema según el plan de seguridad de la organización. 2.1.4. Establece la configuración de los parámetros de red para conectar el servidor según el diseño de red del sistema y los estándares y normas de seguridad y calidad de la organización. 2.1.5. Crea los diferentes grupos y usuarios para permitir la utilización del sistema según las necesidades de la organización y el plan de seguridad del sistema. 2.1.6. Realiza con eficiencia las actualizaciones necesarias del sistema operativo del servidor, asegurando la integridad del sistema, la idoneidad de las mismas y siguiendo las normas de seguridad de la organización. 2.1.7. Refleja en la documentación los detalles relevantes de la instalación, así como las incidencias durante el proceso, según el procedimiento establecido por la organización. 2.1.8. Interpreta la documentación técnica correctamente tanto si está editada en castellano o en las lenguas oficiales de las comunidades autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector. 2.2. Elaborar y mantener inventarios del software del sistema para garantizar su localización y disponibilidad según las normas de la organización. 2.2.1. Enumera el software y sus versiones de forma exhaustiva para mantener un inventario de las aplicaciones y sistemas operativos disponibles en el sistema. 2.2.2. Registra y documenta la configuración actual del software de base y aplicación de forma clara y completa para facilitar las labores de recuperación en caso de fallos. 2.2.3. Enumera la información del software instalado en relación con cada usuario para permitir el control de instalaciones de aplicaciones no permitidas. 2.2.4. Controla el número de instalaciones, su situación e identificación por cada producto software para llevar a cabo un control exhaustivo de licencias cumpliendo la legislación vigente sobre propiedad intelectual. 2.2.5. Registra los privilegios de acceso de los usuarios del sistema a recursos software, para el control de acceso, según el plan de seguridad del sistema y las leyes de datos vigentes. 2.2.6. Utiliza las aplicaciones de inventariado automático para mantener actualizada la información acerca del software del sistema. 2.3. Instalar y configurar aplicaciones corporativas para atender funcionalidades de usuarios según el plan de implantación de la organización 2.3.1. Realiza la instalación del software corporativo asegurando la integridad del sistema, cumpliendo los requisitos establecidos por la organización y siguiendo lo indicado en la documentación técnica. 2.3.2. Realiza la verificación del funcionamiento del software en el conjunto del sistema según los procedimientos de seguridad y calidad establecidos por la organización y el propio fabricante.

2.3.3. Configura el software corporativo con parámetros adecuados según el plan de seguridad del sistema y las necesidades de la organización.
2.3.4. Realiza las actualizaciones necesarias del software corporativo, asegurando la integridad del sistema, la idoneidad de las mismas y siguiendo las normas de seguridad de la organización.
2.3.5. Refleja en la documentación, los detalles relevantes de la instalación, así como las incidencias durante el proceso, según el procedimiento establecido por la organización.
2.3.6. Interpreta correctamente la documentación técnica tanto si está editada en castellano o en las lenguas oficiales de las comunidades autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector.
2.4. Elaborar el plan de soporte a los usuarios, coordinando al personal técnico de apoyo y mantenimiento para asegurar el uso de las funciones del sistema informático.
2.4.1. Documenta de forma exhaustiva las pautas para la instalación, configuración y mantenimiento de software de base y de aplicación en puestos de usuario.
2.4.2. Documenta de forma exhaustiva la resolución de problemas comunes referidos a dispositivos hardware y de red en puestos de usuario.
2.4.3.Planifica la asistencia al usuario aplicando las técnicas de comunicación, los protocolos de actuación establecidos por la organización y siguiendo las políticas de seguridad y protección de datos vigentes y calidad del servicio.
2.4.4. Planifica el entrenamiento de los usuarios en las diferentes herramientas y equipos a manejar para ser realizado de forma asistida y gradual, asegurando su completa adaptación al entorno.
2.4.5. Organiza los procedimientos de asistencia para asegurar su máxima disponibilidad al requerimiento de asesoramiento y atención por parte de los usuarios.
2.5. Configurar y administrar los recursos del sistema para optimizar el rendimiento según los parámetros de explotación de las aplicaciones.
2.5.1. Establece las métricas de rendimiento a utilizar para especificar los atributos de rendimiento a considerar.
2.5.2. Establece las técnicas de análisis del rendimiento a utilizar para la obtención de parámetros de funcionamiento del sistema.
2.5.3. Establece los programas de comprobación a utilizar para obtener parámetros del rendimiento del sistema.
2.5.4. Realiza los modelos que representan al sistema para obtener parámetros del rendimiento del mismo
2.5.5. .Configura los sistemas de simulación del sistema para obtener parámetros del rendimiento del mismo
2.5.6. Analiza los parámetros de rendimiento del sistema obtenidos para localizar posibles conflictos y determinar los dispositivos hardware susceptible de ser reconfigurados, eliminados o añadidos
2.5.7. Reconfigura los componentes hardware, eliminan o añaden de acuerdo al análisis realizado para la mejora del rendimiento de las aplicaciones
2.6. Planificar la realización de copias de seguridad así como la recuperación de las mismas para mantener niveles adecuados de seguridad en los datos según las necesidades de uso y dentro de las directivas de la organización.
2.6.1. Diseña la arquitectura del sistema de copias de respaldo teniendo en cuenta los requisitos del sistema informático.
2.6.2. Planifica los procedimientos de realización de copias de respaldo y los niveles de dichas copias en función de las necesidades del servidor, de los tiempos de realización de las copias, de los tiempos de recuperación, de los espacios de almacenamiento requeridos y de la validez del histórico de copias.
2.6.3. Realiza las pruebas de verificación de las copias de respaldo y se verifica su funcionalidad atendiendo a las especificaciones de calidad de la organización.
2.6.4. Realiza la planificación del sistema de identificación y almacenamiento de los soportes en función de las especificaciones del plan de seguridad de la organización.
2.6.5 Confecciona la documentación de los procedimientos de obtención y verificación de copias de respaldo así como la de los planes de contingencias y resolución de incidencias según la normativa de la organización.
2.7. Auditar la utilización de recursos del sistema para asegurar un rendimiento óptimo según los parámetros del plan de explotación.
2.7.1. Implementa el plan de auditoria con las pruebas funcionales necesarias y periodos de realización, de forma que garanticen el óptimo rendimiento del sistema.
2.7.2. Realiza la comprobación de incidencias para verificar, precisar y minimizar efectos negativos sobre el sistema.
2.7.3. Realiza el diagnóstico y localización de funcionamientos indeseados utilizando los equipos y las herramientas necesarias, y se aplica el correspondiente procedimiento correctivo en un tiempo adecuado.
2.7.4. Realiza el informe de auditoría en el formato normalizado que permita recoger la información requerida para la actuación del repositorio de incidencias.
2.7.5. Interpreta correctamente la documentación técnica tanto si está editada en castellano o en las lenguas oficiales de las comunidades autónomas como si lo está en el idioma extranjero de uso más frecuente en el sector."

		UC3 Asegurar equipos informáticos. 3.1. Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad. 3.1.1. Analiza el plan de implantación del sistema informático de la organización comprobando que incorpora la información necesaria referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones entre otros, así como referencias de posibilidades de utilización de los equipos y restricciones de los mismos y protecciones contra agresiones de virus y otros elementos no deseados. 3.1.2. Determina los permisos de acceso, por parte de los usuarios, a los distintos recursos del sistema por medio de las herramientas correspondientes según el plan de implantación y el de seguridad del sistema informático. 3.1.3. Realiza el acceso a los servidores garantizando la confidencialidad e integridad de la conexión según las normas de seguridad de la organización. 3.1.4. Analiza las políticas de usuario verificando que quedan reflejadas circunstancias tales como usos y restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos. 3.1.5. Transmita la política de seguridad a los usuarios, asegurándose de su correcta y completa comprensión. 3.1.6. Documenta las tareas realizadas convenientemente según los procedimientos de la organización. 3.1.7. Trata las informaciones afectadas por la legislación de protección de datos verificando que los usuarios autorizados cumplan los requisitos indicados por la normativa y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad. 3.2. Configurar servidores para protegerlos de accesos no deseados según las necesidades de uso y dentro de las directivas de la organización. 3.2.1. Realiza la ubicación del servidor en la red en una zona protegida y aislada según la normativa de seguridad y el plan de implantación de la organización. 3.2.2. Activa y configura los servicios que ofrece el servidor desactivando los innecesarios según la normativa de seguridad y plan de implantación de la organización. 3.2.3. Configura los accesos y permisos a los recursos del servidor por parte de los usuarios en función del propósito del propio servidor y de la normativa de seguridad de la organización. 3.2.4. Activa y habilita los mecanismos de registro de actividad e incidencias del sistema los procedimientos de análisis de dichas informaciones. 3.2.5. Analiza los módulos adicionales del servidor en base a sus funcionalidades y riesgos de seguridad que implican su utilización, llegando a una solución de compromiso. 3.2.6. Configura los mecanismos de autenticación para que ofrezcan niveles de seguridad e integridad en la conexión de usuarios de acuerdo con la normativa de seguridad de la organización. 3.2.7. Define y asigna los roles y privilegios de los usuarios siguiendo las instrucciones que figuren en la normativa de seguridad y el plan de explotación de la organización. 3.3. Instalar y configurar cortafuegos en equipos y servidores para garantizar la seguridad ante los ataques externos según las necesidades de uso y dentro de las directivas de la organización. 3.3.1. Selecciona la topología de los cortafuegos en función del entorno de implantación. 3.3.2. Elige los elementos hardware y software del cortafuegos teniendo en cuenta factores económicos y de rendimiento. 3.3.3. Instala y configura los cortafuegos según el nivel definido en la política de seguridad 3.3.4. Determina, configura y administra las reglas de filtrado y los niveles de registro y alarmas según las necesidades dictaminadas por la normativa de seguridad de la organización. 3.3.5. Verifica los cortafuegos con juegos de pruebas y se comprueba que superan las especificaciones de la normativa de seguridad de la organización. 3.3.6. Realiza la instalación y actualización de los cortafuegos y los procedimientos de actuación, con el mismo quedan documentados según las especificaciones de la organización. 3.3.7. Define y configura los sistemas de registro para la revisión y estudio de los posibles ataques, intrusiones y vulnerabilidades.
CAPACIDAD REQUERIDA	**4.1 Capacidades o Habilidades.**	Comprensión oral y escrita Fluidez de ideas (creatividad, innovación) Reconocimiento y solución de problemas Razonamiento inductivo - deductivo Ordenar información Razonamiento lógico/matemático Ubicación espacial
		Introducción al sistema informático Arquitectura de computador Mantenimiento de equipos informáticos Redes de área local (RAL)

4. CAF	**4.2 Conocimiento.**	Redes de área local (RAL) Sistemas operativos Ofimática Bases de datos Programación básica Seguridad informática
5.	**LAS APTITUDES (CUANDO CORRESPONDA).**	NO APLICA
6.	**PRE- REQUISITOS (CUANDO CORRESPONDA).**	**Nivel de Formación:** Bachiller **Experiencia** Para Bachiller técnico: Título de Bachiller Técnico a fin al perfil Para Bachiller: 2 años de experiencia en actividades afines **Capacitación:** N/A
7.	**CÓDIGO DE CONDUCTA (CUANDO CORRESPONDA).**	Será considerado por el OEC, conforme Norma de Reconocimiento SETEC.
8.	**CRITERIOS PARA LA CERTIFICACIÓN.**	1. Cancelar cuota (de ser el caso) 2. Firmar código de ética y conducta determinado por el OEC -de ser el caso-
9.	**MÉTODOS DE EVALUACIÓN INICIAL DE LA CERTIFICACIÓN.**	**Teórico**: Resolución de un banco de preguntas para determinar su conocimiento en el perfil (mínimo 70%). **Práctico**: Resolución de casos / ejercicios prácticos para determinar que posee las competencias del perfil (100%)
10.	**TIEMPO DE VIGENCIA**	3 años
11.	**MÉTODO DE VIGILANCIA (DE SER EL CASO) CRITERIO, TIEMPO, FRECUENCIA,.**	Conforme lo determine el OEC, en función Norma de Reconocimiento.
12.	**CRITERIO PARA SUSPENDER O RETIRAR LA CERTIFICACIÓN**	Norma de Reconocimiento OEC.
13.	**CRITERIOS PARA CAMBIOS DEL ALCANCE DE LA CERTIFICACIÓN DE SER EL CASO.**	Si existe alguna modificación al perfil ocupacional o norma técnica u otro elemento normativo superior, determinado por el Organismo regulador.
14.	**FECHA APROBACIÓN DEL ESQUEMA.**	**13/7/2017**