Asunto: **Revisión de subsanación solvencia técnica Deloitte**
Exte: S-00597-2024. Soporte implantación SGSI y adecuación a ENS

En relación con el nuevo modelo de declaración responsable presentado por la firma Deloitte de fecha de 22 de mayo de 2024, manifestando que cuenta con la Certificación CMMi Nivel 3 y aportando a estos efectos tabla comparativa, se ha realizado la correspondiente prueba de contraste entre ambas normas; ISO 9001, ISO 20000, y la descripción de CCMI aportada por la empresa Deloitte.

También se considera la pretensión relativa a la complementariedad de la certificación Leet Security para cubrir los dominios no cubiertos por la ISO 20000, respecto de lo cual se debe señalar que Leet Security se ajusta exclusivamente a evaluar los niveles de seguridad implementados en las dimensiones de Confidencialidad, Integridad y Disponibilidad respecto de la seguridad, y no de la gestión del ciclo de vida del servicio. Para ello usa métricas con la que valora el posicionamiento dichas dimensiones, pero no acredita el cumplimiento de los controles, sino que pone una calificación sobre su cumplimiento.

En cuanto a la certificación SOC 2 Level 2, el cumplimiento está dirigido al examen de los controles relativos al manejo de la información sensible, bajo los criterios de seguridad, disponibilidad, integridad, confidencialidad y privacidad, informando del cumplimiento sobre un periodo de tiempo que cubre el diseño, implementación y efectividad operativa de los controles, incluyendo la descripción del sistema, el diseño de los controles y las pruebas de la eficacia operativa de los controles. Todo ello respecto de la seguridad de la información, no de la gestión del ciclo de vida de la gestión del servicio tal y como es tratada en la ISO 20000.

En este sentido, el contraste se ha realizado desde la perspectiva de su enfoque de implementación teniendo en cuenta que la ISO/IEC 20000 se enfoca en establecer y mantener un sistema de gestión de servicios de TI que cubra todas las etapas del ciclo de vida del servicio a nivel Corporativo, mientras que CMMI Nivel 3, requiere la definición y gestión de procesos organizativos estándar y su personalización para proyectos específicos. El contraste de equivalencias realizado se plantea teniendo en cuenta los dominios y subdominios de las normas citadas, en la cual se detectan ausencias de controles equivalentes que se reflejan en la siguiente tabla:

Dominio	Subdominio	ISO 20000	ISO 9001	CMMI
Introducción		X	X	
Objeto	Generalidades	X	X	
	Campo de aplicación	X	X	
Normas		X	X	
Términos	Términos específicos a las normas de sistemas de gestión	X	X	
	Términos específicos a la gestión de servicios	X		
Contexto	Compresión de la organización y su contexto	X	X	
	Comprensión de las necesidades y expectativas de las partes	X	X	
	Determinación del alcance de sistema de gestión de servicios	X	X	
	Sistema de gestión de servicios	X		
Liderazgo	Liderazgo y compromiso	X	X	
	Política de gestión de servicios	X		
	Establecer política de gestión de servicios	X		
	Comunicar la política de gestión de servicios	X		
	Roles, responsabilidades y autoridades en la organización	X	X	
Planificación	Acciones para tratar riesgos y oportunidades	X	X	
	Objetivos de gestión de servicios y planificación para su consecución	X	X	
	Establecer objetivos	X		
	Planificar la consecución de objetivos	X		
	Planificar el sistema de gestión de servicios	X	X	
Apoyo	Recursos	X	X	
	Competencias	X	X	
	Concienciación	X		
	Comunicación	X	X	
	Información documentada	X	X	

	Generalidades	X	X	
	Creación y actualización de la información documentada	X	X	
	Control de la información documentada	X	X	
	Información documentada del sistema de gestión del servicio	X		
	Conocimiento	X	X	X
Operación	Planificación y control operacional	X	X	
	Porfolio de servicios	X		
	Prestación de servicios	X		
	Planificación de servicios	X	X	
	Control de partes involucradas en el ciclo de vida de los servicios	X	X	
	Gestión de catálogo de servicios	X		
	Gestión de activos	X		
	Gestión de la configuración	X		X
	Relación y acuerdo	X		
	Generalidades	X	X	
	Gestión de relaciones con el negocio	X		X
	Gestión de niveles de servicio	X		X
	Gestión de proveedores	X	X	X
	Oferta y demanda	X		
	Presupuesto y contabilidad de servicios	X		X
	Gestión de la demanda	X	X	X
	Gestión de la capacidad	X		X
	Diseño, construcción y transición de servicios	X		
	Gestión de cambios	X	X	X
	Diseño y transición de servicios	X		
	Gestión de entregas y despliegues	X		
	Resolución y ejecución	X		
	Gestión de incidencias	X		X
	Gestión de peticiones de servicio	X		
	Gestión de problemas	X		X
	Aseguramiento de servicios	X		
	Gestión de la disponibilidad de los servicios	X		X
	Gestión de la continuidad de los servicios	X		X
	Gestión de la seguridad de la información	X		X
Evaluación	Evaluación del desempeño	X	X	
	Monitorización, medición, análisis y evaluación	X	X	
	Auditoría interna	X	X	
	Revisión por la dirección	X	X	
	Informes de servicio	X		
Mejora	No conformidad y acción correctiva	X	X	
	Mejora continua	X	X	

La memoria justificativa que se desarrolló sobre la base del artículo 28 de la Ley de Contratos del Sector Publico, consideró imprescindibles las certificaciones al estar directamente relacionadas con la claridad y garantías de seguridad con las que tiene que proporcionar las prestaciones objeto del expediente:

- Desde la perspectiva de seguridad a través de las ISO 22301, 27001 y ENS nivel medio o alto.
- Desde una perspectiva de claridad/gestión, a través de las ISO 9001 y 20000. Abundando en el contenido de las normas, el objeto de la ISO 9001 es cumplir con las expectativas de los clientes y demostrar su compromiso con la calidad. Sin embargo, la ISO 20000 su ámbito es más concreto y especifico, suplementando y alineando a su vez con la naturaleza de los servicios objeto del contrato, consistente en obtener unos servicios bien planificados, diseñados, administrados y entregados en el ámbito de las tecnologías de la información.

Los certificados requeridos en el pliego son un modo de acreditar la solvencia técnica y profesional de los licitadores y su idoneidad para la ejecución del proyecto.

La solicitud de cumplimiento de las normas requeridas (incluyendo la norma ISO/IEC 20000), y los certificados que las acreditan, están vinculados al objeto del contrato y a las especificaciones técnicas incluidas en los pliegos

No se trata de un requisito "sien qua nom" dado que el propio pliego recoge y admite que dichos certificados pueden ser sustituidas por otros equivalentes.

La exigencia de los certificados no puede considerarse restrictivos para la concurrencia y menos aún discriminatorios dado que las norma ISO son las de mayor difusión, reconocimiento y aceptación nacional e internacional, especialmente en la Unión Europea.

Significar que la oferta de la empresa Deloitte es la única que no aporta certificación de cumplimiento de la norma ISO/IEC 20000, mientras que el resto de ofertas (cuatro) si disponen de dicha certificación.

Podemos concluir que, las certificaciones de la empresa Deloitte pueden aportar un nivel adecuado para la mejora de los procesos y la gestión de la calidad, pero en su conjunto no pueden sustituir los controles de la norma ISO/IEC 20000 debido a la especificidad de esta última que orienta todos sus procesos a servicios TI.

La certificación ofertada por Deloitte no puede considerase equivalente debido a sus diferencias de enfoque, propósito o ámbito de aplicación, y por lo tanto no acredita el mismo nivel de garantía y estándares de calidad que los certificados que se requieren en los pliegos.