

## **Consultas Realizadas**

### **Licitación 466419 - MCN Nº 07/25 - ADQUISICION DE EQUIPOS INFORMATICOS**

## Consulta 1 - CAPACIDAD TECNICA

Consulta	Fecha de Consulta	29-04-2025
<p>Consultamos a la Convocante cual es el criterio para realizar el direccionamiento a empresas que poseen la certificación ISO 27001/22 atendiendo a que esta licitación corresponde a la provisión de equipos informáticos adquiridos desde un representante legal autorizado por el fabricante. La norma ISO/IEC 27001 es la norma más conocida a nivel mundial para sistemas de gestión de la seguridad de la información, por ende los proveedores no administraran información de los equipos, si no proveerán los equipos para que sean administrados por la convocante. Solicitamos modificar este requerimiento que puede entenderse por un direccionamiento, a fin de que mas proveedores pueda participar y así la convocante tenga mas posibilidades de elección.</p>		

Respuesta	Fecha de Respuesta	09-05-2025
<p>Las certificaciones ISO 27001 o superiores son exigidas para asegurar que las empresas implementen un sistema robusto de gestión de seguridad de la información, protegiendo la confidencialidad e integridad de los datos sensibles. Obtener esta certificación demuestra el compromiso de la organización con estándares internacionales, garantizando procesos auditados periódicamente y ofreciendo una mayor confianza en su capacidad para manejar información crítica, como es el caso de los equipos informáticos a ser adquiridos en esta licitación. Este requisito busca asegurar la calidad y protección de la información, alineándose con los principios de eficiencia y economía en la contratación pública.</p> <p>La inclusión de la certificación ISO 27001 o superior en los pliegos de licitación, respaldada por la DNCP, no se considera una limitación para los oferentes. Se aceptan certificaciones superiores que cumplan con los mismos criterios de seguridad de la información. Este requisito ya ha sido aplicado en procesos anteriores, destacando la importancia de que los proveedores, especialmente en el soporte de equipos destinados al manejo de información sensible, demuestren un compromiso continuo con la seguridad y confidencialidad de los datos durante el período de garantía. Ref: Resolución DNCP N° 3440/24.</p> <p>El requisito de Garantía de los equipos, tal cual lo solicita en el apartado 22 del ítem 1 y en el apartado 25 del ítem 2, "La Garantía (escrita): Mínimo 36 meses. Incluye: Soporte de atención de Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.</p> <p>Durante este periodo de garantía el oferente deberá dar Soporte de atención de Hardware, Mano de Obra, Repuesto y traslado desde la institución a su oficina, lo que implica que el mismo tendrá acceso a los equipos con información clasificada que debe ser manejada con mucha seguridad, razón por la cual es requerida la Certificación ISO 27001:2022 similar o superior, de manera a garantizar la confidencialidad de la información a la que tendrán acceso.</p> <p>Es importante señalar que conforme a plantilla estándar emitida por MITIC y también a la autorización con que cuenta el presente llamado por dicha Institución, que dicha garantía brindara a la Convocante una confianza plena de que toda la información sensible que se encuentre en los equipos que pudieran presentar fallas y necesiten ser trasladadas para su reparación, será bajo resguardo, responsabilidad y seguridad del oferente.</p> <p>Esto se funda en que el Consejo de Defensa Nacional maneja información altamente sensible y confidencial. La certificación ISO 27001:2022 similar o superior garantiza que los procesos de soporte técnico y la gestión de seguridad del hardware están diseñados para proteger esa información contra accesos no autorizados, pérdida, filtraciones o daño. Esta norma establece un marco para implementar medidas de seguridad adecuadas, evaluarlas y mantenerlas efectivas.</p> <p>La implantación de la ISO 27001 es la respuesta ideal a los requisitos legislativos y de los clientes, incluyendo el RGPD y otras amenazas potenciales, incluyendo: Crimen cibernético, violación de los datos personales, vandalismo / terrorismo, fuego / daños, uso malintencionado, robo y ataque de virus.</p> <p>Los equipos adquiridos en este proceso serán destinados a funcionarios de altos mandos que manejan información muy sensible del ESTADO PARAGUAYO, razón por la cual, la seguridad de la información es crítica ya que en caso de fallas y/o reparación, el proveedor deberá tener conocimiento y realizar las prácticas de resguardo de la información, considerando de que filtraciones de datos podría ocasionar un terrible problema a nivel nacional como internacional.</p> <p>Cabe aclarar que no solo es aceptada la Certificación ISO 27001:2013, también serán aceptadas certificaciones similares o superiores conforme se desprende el requisito de Capacidad técnica.</p>		

## Consulta 2 - Capacidad Financiera

Consulta	Fecha de Consulta	29-04-2025
Solicitamos respetuosamente a la Convocante aceptar la Capacidad Financiera de los años 2022, 2023 y 2024.		

Respuesta	Fecha de Respuesta	09-05-2025
En referencia a la consulta realizada, se pone a conocimiento que la Convocante considera mantenerse en lo establecido inicialmente, teniendo en cuenta la Resolución General Nº 29/25 de la Dirección Nacional de Ingresos y Tributación, por la cual se prorroga los plazos para la presentación de los estados financieros correspondientes al ejercicio fiscal 2024.		

## Consulta 3 - Capacidad técnica

Consulta	Fecha de Consulta	02-05-2025
<p>El alcance de la ISO 27001:2022 descrito en el PBC limita injustificadamente la participación de otros oferentes que cuentan con la certificación ISO 27001:2022 vigente y plenamente válida, con un alcance similar pero no exactamente idéntico, aunque igualmente relacionado a servicios de soporte técnico, gestión de seguridad de la información y tecnología.</p> <p>Consideramos que al restringir el alcance únicamente a "Servicio de Soporte técnico y de seguridad de hardware del área de Tecnología para el Sector Público" se incurre en una especificación direccionada y no permite la libre competencia.</p> <p>Solicitamos respetuosamente que dicho requisito sea modificado o eliminado, de manera a permitir la participación de proveedores que cuenten con certificación ISO 27001:2022 con alcances pertinentes y relacionados, conforme a los estándares internacionales de gestión de seguridad de la información, sin limitarla a un alcance específico que favorezca únicamente a ciertos proveedores.</p>		

Respuesta	Fecha de Respuesta	09-05-2025
<p>Las certificaciones ISO 27001 o superiores son exigidas para asegurar que las empresas implementen un sistema robusto de gestión de seguridad de la información, protegiendo la confidencialidad e integridad de los datos sensibles. Obtener esta certificación demuestra el compromiso de la organización con estándares internacionales, garantizando procesos auditados periódicamente y ofreciendo una mayor confianza en su capacidad para manejar información crítica, como es el caso de los equipos informáticos a ser adquiridos en esta licitación. Este requisito busca asegurar la calidad y protección de la información, alineándose con los principios de eficiencia y economía en la contratación pública.</p> <p>La inclusión de la certificación ISO 27001 o superior en los pliegos de licitación, respaldada por la DNCP, no se considera una limitación para los oferentes. Se aceptan certificaciones superiores que cumplan con los mismos criterios de seguridad de la información. Este requisito ya ha sido aplicado en procesos anteriores, destacando la importancia de que los proveedores, especialmente en el soporte de equipos destinados al manejo de información sensible, demuestren un compromiso continuo con la seguridad y confidencialidad de los datos durante el período de garantía. Ref: Resolución DNCP N° 3440/24.</p> <p>El requisito de Garantía de los equipos, tal cual lo solicita en el apartado 22 del ítem 1 y en el apartado 25 del ítem 2, "La Garantía (escrita): Mínimo 36 meses. Incluye: Soporte de atención de Hardware, Mano de Obra y Repuestos incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor.</p> <p>Durante este periodo de garantía el oferente deberá dar Soporte de atención de Hardware, Mano de Obra, Repuesto y traslado desde la institución a su oficina, lo que implica que el mismo tendrá acceso a los equipos con información clasificada que debe ser manejada con mucha seguridad, razón por la cual es requerida la Certificación ISO 27001:2022 similar o superior, de manera a garantizar la confidencialidad de la información a la que tendrán acceso.</p> <p>Es importante señalar que conforme a plantilla estándar emitida por MITIC y también a la autorización con que cuenta el presente llamado por dicha Institución, que dicha garantía brindara a la Convocante una confianza plena de que toda la información sensible que se encuentre en los equipos que pudieran presentar fallas y necesiten ser trasladadas para su reparación, será bajo resguardo, responsabilidad y seguridad del oferente.</p> <p>Esto se funda en que el Consejo de Defensa Nacional maneja información altamente sensible y confidencial. La certificación ISO 27001:2022 similar o superior garantiza que los procesos de soporte técnico y la gestión de seguridad del hardware están diseñados para proteger esa información contra accesos no autorizados, pérdida, filtraciones o daño. Esta norma establece un marco para implementar medidas de seguridad adecuadas, evaluarlas y mantenerlas efectivas.</p>		

La implantación de la ISO 27001 es la respuesta ideal a los requisitos legislativos y de los clientes, incluyendo el RGPD y otras amenazas potenciales, incluyendo: Crimen cibernético, violación de los datos personales, vandalismo / terrorismo, fuego / daños, uso malintencionado, robo y ataque de virus.

Los equipos adquiridos en este proceso serán destinados a funcionarios de altos mandos que manejan información muy sensible del ESTADO PARAGUAYO, razón por la cual, la seguridad de la información es crítica ya que en caso de fallas y/o reparación, el proveedor deberá tener conocimiento y realizar las prácticas de resguardo de la información, considerando de que filtraciones de datos podría ocasionar un terrible problema a nivel nacional como internacional.

Cabe aclarar que no solo es aceptada la Certificación ISO 27001:2013, también serán aceptadas certificaciones similares o superiores conforme se desprende el requisito de Capacidad técnica.

## Consulta 4 - Especificaciones técnicas / ITEM 1 - Computadoras de Escritorio - Intermedia

Consulta	Fecha de Consulta	05-05-2025
Referente al punto que establece como requisito "1 (un) puerto USB Tipo C 3.2 Gen 1 o superior como mínimo", se consulta a la Convocante si se aceptará el cumplimiento de dicho requerimiento mediante el uso de adaptadores USB-C a USB-A o mediante expansión vía tarjeta PCI Express, considerando que ambas opciones permiten ofrecer la funcionalidad solicitada sin afectar el rendimiento ni la compatibilidad del equipo.		

Respuesta	Fecha de Respuesta	09-05-2025
En referencia a la consulta realizada, se manifiesta que las EETT son emitidas y aprobadas por MITIC, que son estándares establecidos por la Institución competente, por lo que se solicita que todo potencial oferente se ajuste a lo establecido inicialmente por la Convocante en el PBC.		