

OBJETO: “RENOVAR EL SOPORTE Y LICENCIAMIENTO DE LOS EQUIPOS FORTINET (FORTIGATE, FORTIANALYZER Y FORTIMANAGER), INCLUYENDO LOS SERVICIOS DEL FABRICANTE (FORTICARE Y FORTIGUARD), ACTUALIZACIONES DE SEGURIDAD, SOPORTE ESPECIALIZADO 5X8 PARA LA ATENCIÓN DE INCIDENTES Y ACOMPAÑAMIENTO EN LA OPERACIÓN DE LA INFRAESTRUCTURA, GARANTIZANDO LA CONTINUIDAD OPERATIVA, LA PROTECCIÓN PERIMETRAL Y EL CUMPLIMIENTO DE LOS LINEAMIENTOS TÉCNICOS Y DE CIBERSEGURIDAD DEL INSTITUTO DISTRITAL DE LAS ARTES - IDARTES.”.

OFERENTE INTERESADO:	INNDOT SAPI DE CV
----------------------	-------------------

OBSERVACIÓN 1:

OBS 1:

De manera respetuosa, se solicita a la Entidad incorporar el siguiente requisito con el propósito de asegurar que el proponente disponga del respaldo, experiencia y nivel de especialización necesarios para la adecuada ejecución del proyecto. Lo anterior permitirá garantizar que la solución ofrecida cuente con el acompañamiento directo del fabricante y que la Entidad obtenga el máximo aprovechamiento de la plataforma tecnológica implementada.

Requisito propuesto:

El oferente deberá acreditar, como mínimo, las especializaciones o competencias de partner otorgadas por la marca propuesta, demostrando capacidades avanzadas en diseño, implementación, administración y soporte de soluciones de seguridad, específicamente en las siguientes áreas:

- SD-WAN
- Secure Networking (LAN)
- Security Operations

Para acreditar el cumplimiento de este requisito, el proponente deberá adjuntar junto con su oferta la certificación expedida por el fabricante, emitida a nombre del oferente y con fecha de expedición no superior a treinta (30) días calendario anteriores al cierre del proceso.

La inclusión de esta exigencia permitirá a la Entidad contar con proveedores que acrediten conocimientos especializados y respaldo directo del fabricante, garantizando una implementación eficiente, una operación segura y una adecuada gestión de la infraestructura tecnológica durante toda la ejecución contractual.

RESPUESTA 1:

La Entidad agradece la observación. No obstante, el objeto del presente proceso se limita a la renovación de soporte y licenciamiento de equipos Fortinet ya instalados y en operación en el IDARTES, sin que se contemple diseño, implementación o modificación de la infraestructura existente. En consecuencia, las especializaciones propuestas resultan desproporcionadas frente al alcance contractual. La certificación como partner Expert del programa Fortinet Engage Partner Program, ya exigida en el numeral 2.2.3 del pliego, es suficiente y adecuada para garantizar el respaldo del fabricante. **La observación no es acogida.**

OBSERVACIÓN 2:

OBS 2 :

De manera respetuosa, solicitamos a la Entidad evaluar la incorporación del siguiente requisito, con el fin de garantizar que los proveedores cuenten con las capacidades técnicas, experiencia y buenas prácticas necesarias para la adecuada gestión de la seguridad de la información durante la ejecución del contrato.

Requisito propuesto:

El oferente deberá demostrar que sus procesos y procedimientos se encuentran alineados con las políticas de seguridad definidas por la Entidad y con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI)

promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Para ello, deberá acreditar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) certificado bajo estándares internacionales vigentes, aplicable a los servicios objeto del contrato, incluyendo actividades relacionadas con la administración, soporte, monitoreo y mejora continua de los servicios de tecnologías de la información.

Como soporte de este requisito, el proponente deberá presentar junto con su oferta una copia de la certificación correspondiente, expedida por un organismo certificador acreditado y vigente a la fecha de presentación de la propuesta.

La incorporación de esta exigencia permitirá a la Entidad contar con proveedores que operen bajo marcos de gestión reconocidos internacionalmente, garantizando la aplicación de controles adecuados para la protección de la información, la gestión de riesgos, la continuidad de los servicios y el cumplimiento de las mejores prácticas en materia de ciberseguridad y protección de datos.

RESPUESTA 2:

La Entidad agradece la observación. Si bien la gestión de seguridad de la información es un aspecto relevante, la exigencia de una certificación bajo estándares internacionales de SGSI constituiría una barrera de acceso desproporcionada respecto del valor y naturaleza del contrato, que corresponde exclusivamente a renovación de licencias y soporte del fabricante. Dicha exigencia podría restringir la pluralidad de oferentes en contravía del principio de selección objetiva establecido en la Ley 80 de 1993. La observación **no es acogida**.

OBSERVACIÓN 3:

OBS 3:

De manera respetuosa, solicitamos a la Entidad evaluar la inclusión del siguiente requisito, con el propósito de garantizar que los servicios objeto del contrato sean prestados bajo estándares reconocidos de calidad, eficiencia operativa y mejora continua, contribuyendo al cumplimiento de los niveles de servicio requeridos.

Requisito propuesto:

El oferente deberá acreditar que cuenta con una mesa de servicios (Service Desk) o centro de soporte certificado bajo un estándar internacional vigente para la gestión de servicios de tecnologías de la información, aplicable a las actividades de soporte, atención de incidentes, requerimientos y operación de servicios relacionados con el objeto contractual.

Para acreditar el cumplimiento de esta condición, el proponente deberá adjuntar con su oferta la certificación correspondiente, emitida por un organismo certificador reconocido y vigente al momento de la presentación de la propuesta.

La incorporación de este requisito permitirá a la Entidad contar con proveedores que operen bajo metodologías estructuradas y buenas prácticas internacionalmente aceptadas para la gestión de servicios de TI, asegurando una atención oportuna, procesos de soporte estandarizados, seguimiento efectivo de los requerimientos y una mejora permanente en la prestación de los servicios contratados.

RESPUESTA 3:

La Entidad agradece la observación. El objeto contractual contempla soporte especializado 5x8 para atención de incidentes sobre los equipos Fortinet del IDARTES, actividad que no requiere la acreditación de una mesa de servicios certificada bajo estándares internacionales de gestión de TI, pues ello excede el alcance y valor del proceso. Exigir dicha certificación impondría requisitos adicionales no proporcionales a la naturaleza del contrato y limitaría indebidamente la competencia. **La observación no es acogida**.

OBSERVACIÓN 4:

OBS 4:

De manera respetuosa, solicitamos a la Entidad considerar la incorporación del siguiente requisito, orientado a garantizar que el proveedor cuente con capacidades especializadas para la gestión, atención y respuesta de incidentes de seguridad de la información, fortaleciendo así la protección de los activos tecnológicos y la continuidad de los servicios contratados.

Requisito propuesto:

El oferente deberá demostrar que dispone de procesos, metodologías y procedimientos formalmente definidos para la gestión de incidentes de seguridad de la información, alineados con estándares y mejores prácticas reconocidas internacionalmente. Para tal fin, deberá acreditar la implementación de un sistema certificado que contemple actividades de identificación, análisis, tratamiento, respuesta y mejora continua frente a incidentes de seguridad informática.

Como soporte de este requisito, el proponente deberá aportar junto con su oferta una certificación vigente expedida por un organismo acreditado, que evidencie la adopción de controles y procedimientos específicos para la gestión de incidentes de seguridad de la información. Dicha certificación deberá encontrarse alineada con las políticas institucionales de seguridad y con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

La incorporación de esta exigencia permitirá a la Entidad contar con proveedores que dispongan de mecanismos formales y estructurados para la atención de eventos de seguridad, reduciendo riesgos operacionales, fortaleciendo la protección de la información institucional y asegurando la disponibilidad, integridad y continuidad de los servicios objeto del contrato.

RESPUESTA 4:

La Entidad agradece la observación. Los requerimientos técnicos del presente proceso han sido definidos con base en el estudio del sector y son proporcionales al objeto contractual, que consiste en la renovación de soporte y licenciamiento de equipos Fortinet. La exigencia de una certificación formal en gestión de incidentes de seguridad resulta ajena al alcance del contrato y generaría restricciones injustificadas a la participación de proponentes, afectando los principios de transparencia y pluralidad. **La observación no es acogida.**

OFERENTE INTERESADO:

EYC INGENIEROS

OBSERVACIÓN 1:

1	Anexo Tecnico Fortinet 5. OBLIGACIONES ESPECIFICAS 3. Prestar soporte técnico especializado en modalidad 5x8, con atención virtual prioritaria y presencial únicamente cuando sea requerido por la Entidad.	De la manera más atenta, solicitamos a la entidad que considere agregar el siguiente ítem al proceso, con el objetivo de asegurar que los servicios prestados por los oferentes sean de la más alta calidad, gestionados eficientemente y con un enfoque constante en la mejora continua. ITEM: "El oferente debe contar con una mesa de servicios y/o mesa de ayuda que esté certificada bajo la norma internacional vigente del Sistema de Gestión de Servicios en su versión más reciente, aplicable a los procesos de seguridad y soporte de servicios. Esta certificación asegurará la calidad, gestión y mejora continua de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida directamente al oferente por el ente certificador autorizado." Al incluir este requisito, se asegura de que los oferentes estén comprometidos con altos estándares de calidad y gestión, lo que redundará en una prestación de servicios de TI más eficiente y segura, beneficiando así a la entidad en su conjunto.
---	--	--

RESPUESTA 1:

La Entidad agradece la observación. El objeto del presente proceso se circunscribe a la renovación de soporte y licenciamiento de equipos Fortinet ya instalados, sin que se contemple la prestación de servicios administrados de TI de amplio espectro. Exigir una certificación de sistema de gestión de servicios resulta desproporcionado frente al alcance y valor del contrato, y podría restringir indebidamente la participación de proponentes en contravía del principio de selección objetiva. **La observación no es acogida.**

OBSERVACIÓN 2:

2	Anexo Tecnico Fortinet 5. OBLIGACIONES ESPECIFICAS 8. Cumplir con las normas técnicas y legales aplicables en materia de seguridad de la información, protección de datos y ciberseguridad, conforme a lo establecido por el marco normativo vigente en Colombia.	De la manera más atenta, solicitamos a la entidad considerar la inclusión del siguiente requisito, con el objetivo de asegurar que los prestadores de servicios cuenten con la experiencia y la idoneidad necesarias en la gestión de la seguridad de la información: ITEM: "El oferente deberá alinearse a las políticas de seguridad de la entidad, así como el modelo MSP del Ministerio de las Telecomunicaciones de Colombia – Mintic, el prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Seguridad de la Información en su versión más reciente para los procesos relacionados con seguridad y mesa de servicios, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente." Incluir este requisito garantiza que los oferentes tienen un sistema de seguridad de la información sólido y en conformidad con estándares internacionales. Esta certificación asegura que el proveedor ha establecido y mantiene prácticas efectivas para proteger datos sensibles y garantizar la continuidad y confiabilidad de los servicios ofrecidos.
---	--	---

RESPUESTA 2:

La Entidad agradece la observación. Si bien el cumplimiento de las normas de seguridad de la información es una obligación del contratista conforme al numeral 8 de las obligaciones específicas del pliego, la exigencia de una certificación formal bajo estándares internacionales de SGSI constituye una barrera de acceso desproporcionada respecto del valor y naturaleza del contrato. **La observación no es acogida.**

OBSERVACIÓN 3:

3	Anexo Tecnico Fortinet 8. PLAZO 2. Servicios de soporte técnico por demanda: Atención técnica especializada para garantizar el correcto funcionamiento de los equipos Fortinet durante la vigencia del contrato (12 meses).	De la manera más atenta, solicitamos a la entidad que considere este ítem en el siguiente ítem del proceso, con el objetivo de fortalecer las capacidades técnicas y operativas del proveedor en la atención oportuna y eficaz de incidentes de seguridad de la información. La incorporación de este requisito permitirá asegurar que los Servicios Administrados del oferente actúe conforme a estándares internacionales, brindando una respuesta estructurada y alineada con las políticas de seguridad definidas por la entidad y con los marcos de referencia nacionales. ITEM: "El oferente deberá garantizar que los Servicios Administrados cuente con procedimientos formalmente establecidos, documentados y operativos para la gestión de incidentes de seguridad de la información. Para ello, el oferente deberá contar con certificación vigente en la norma Gestión de Incidentes de Seguridad de la Información, la cual establece las mejores prácticas para el tratamiento de incidentes en todo su ciclo de vida: preparación, detección, evaluación, respuesta y aprendizaje. Esta certificación respaldará el cumplimiento de estándares internacionales en la gestión de incidentes, conforme a las políticas de seguridad de la entidad y en armonía con el Modelo de Seguridad y Privacidad de la Información (MSPi) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – MinTIC. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente." La inclusión de este ítem asegurará que los servicios ofrecidos cuenten con un marco formal de actuación ante incidentes, permitiendo mitigar riesgos operativos, proteger los activos de información y garantizar la disponibilidad y continuidad de los servicios críticos contratados.
---	--	---

RESPUESTA 3:

La Entidad agradece la observación. La gestión de incidentes sobre los equipos Fortinet del IDARTES está cubierta por las obligaciones específicas del contrato y por el respaldo del fabricante, garantizado mediante la certificación de partner Expert ya exigida en el numeral 2.2.3 del pliego. Requerir adicionalmente una certificación formal en gestión de incidentes excede el alcance del objeto contractual y limitaría sin justificación suficiente la pluralidad de oferentes. **La observación no es acogida.**

OBSERVACIÓN 4:

4	Anexo Tecnico Fortinet 5. OBLIGACIONES ESPECIFICAS	De manera atenta, se solicita a la entidad incluir el siguiente ítem con el objetivo de garantizar que el oferente cuente con las capacidades necesarias, a nivel de partner, para ejecutar proyectos Fortinet. Esto asegurará que la solución propuesta esté respaldada por el fabricante y que la entidad obtenga el máximo valor en la configuración y gestión de su infraestructura bajo este esquema: ITEM: El oferente deberá contar, como mínimo, con especializaciones de partner de la marca ofertada, con el fin de garantizar que sus procesos cuenten con la mayor capacidad técnica y experiencia en la implementación y operación de soluciones de seguridad y redes, en las siguientes áreas: SD-WAN Secure Networking (LAN) Security Operations El proponente deberá anexar la certificación del fabricante junto a su propuesta, la cual debe ser expedida a nombre de la entidad y tener una fecha de expedición no superior a 30 días. La inclusión de este requisito permitirá asegurar que los oferentes cuenten con la capacidad técnica y el respaldo del fabricante para diseñar, implementar y gestionar infraestructuras Fortinet de manera óptima, maximizando la eficiencia y seguridad de la red de la entidad.
---	--	--

RESPUESTA 4:

La Entidad agradece la observación. El proceso tiene por objeto la renovación de soporte y licenciamiento sobre equipos Fortinet existentes, sin que se contemple diseño, implementación o modificación de infraestructura. La certificación como partner Expert del programa Fortinet Engage Partner Program, ya requerida en el numeral 2.2.3, garantiza suficientemente el respaldo técnico del fabricante para el alcance contratado. Las especializaciones adicionales propuestas resultan ajenas al objeto y desproporcionadas frente al valor del proceso. **La observación no es acogida.**

OBSERVACIÓN 5:

5	Anexo Tecnico Fortinet	De la manera más atenta, solicitamos a la entidad considerar la inclusión del siguiente requisito, con el objetivo de asegurar que el personal asignado al proyecto cuente con las competencias y la experiencia necesarias para llevar a cabo las tareas de manera eficiente y efectiva:
		PERSONAL
		PROFESIONAL DE IMPLEMENTACION
		Ingeniero electrónico, sistemas o telecomunicaciones o afines
		Especialización en seguridad informática
		Mínimo cuatro (4) años de experiencia general a partir de la T.P. y(2) años de experiencia específica en proyectos de seguridad informática, esta será acreditada mediante certificaciones de experiencia laboral.
		ITIL V4 FOUNDATION
		Certificación auditor interno 27001:2013 o superior
		Certified Solution Specialist Network Security
		Certified Professional Security Operations
		Certified Professional Network Security
		PROFESIONAL DE APOYO DE SEGURIDAD INFORMATICA
		Ingeniero de sistemas o carreras a fines
		Especialización en seguridad informática
		Mínimo Seis (6) años de experiencia general todas contadas a partir de la expedición de la T.P., y mínimo tres (3) años de experiencia específica en proyectos de seguridad informática, mediante la presentación de certificaciones laborales y/o contratos.
		Certificación de capacitación como experto en pentest y Vulnerabilidades"
		Certificación básica o avanzada de la marca ofertada
		GERENTE DEL PROYECTO
		Pregrado: Ingeniero electrónico, de sistemas, de telecomunicaciones o afines;
		Posgrado: Especialización y/o Master en gerencia de proyectos y/o en diseño y gestión de proyectos tecnológicos
		EXPERIENCIA: Mínimo ocho (8) años de experiencia general a partir de la T.P. y (5) años de experiencia específica en proyectos de tecnología como Gerente de Proyectos, esta será acreditada mediante certificaciones de experiencia laboral.
		CERTIFICACIONES REQUERIDAS El profesional postulado debe contar con la totalidad de las certificaciones que se relacionan a continuación):
ITIL V4 FOUNDATION		
SCRUM MÁSTER		
ISO/IEC 27001:2022 Auditor interno		
PMP VIGENTE		

RESPUESTA 5:

La Entidad agradece la observación. Los perfiles de personal propuestos —incluyendo gerente de proyecto, profesional de implementación y profesional de apoyo en seguridad, con certificaciones como PMP, SCRUM Master, ITIL V4, ISO 27001 auditor interno y certificaciones Fortinet avanzadas— corresponden a proyectos de implementación o gestión de infraestructuras de mayor envergadura y complejidad. El presente contrato se limita a la renovación de licencias y soporte existente, por lo que dichas exigencias resultan manifiestamente desproporcionadas frente al objeto y valor del proceso, y restringirían injustificadamente la concurrencia de oferentes. **La observación no es acogida.**



Jorge Ramírez
Contratista – OAP- TI



Jonathan González
Profesional Universitario – OAP- TI



Claudia Mendoza
Contratista – OAP- TI



Andrea Díaz Londoño
Contratista – SAF