



HOSPITAL MILITAR CENTRAL
ÁREA GESTIÓN CONTRATOS

FORMULARIO N°. 01 DE OBSERVACIONES Y RESPUESTAS PROCESO LP-007-2026-HOMIL

OBJETO: “ADQUISICIÓN DE LA SUSCRIPCIÓN, ACTUALIZACIÓN DEL LICENCIAMIENTO Y SOPORTE DE LA SOLUCIÓN DE FORTINET DEL HOSPITAL MILITAR CENTRAL”.

El comité estructurador, procede a emitir respuesta oportuna a las observaciones realizadas por los oferentes dentro del proceso de selección de la referencia de la siguiente manera:

OBSERVACIONES FORMULADAS POR ECOMIL SAS.

OBSERVACIÓN No. 1

OBSERVACIÓN – SOLICITUD DE NIVEL DE MEMBRESÍA EXPERT DEL FABRICANTE FORTINET

Respetuosamente solicitamos al HOSPITAL MILITAR CENTRAL modificar el requisito relacionado con la acreditación como Partner autorizado de Fortinet, estableciendo que el oferente deberá contar con membresía vigente nivel Expert, correspondiente al nivel más alto del programa Engage Partner. Exigir únicamente la condición genérica de “Partner” permite la participación de integradores con diferentes niveles de especialización y capacidad técnica, situación que, considerando la criticidad de la infraestructura tecnológica y de ciberseguridad del Hospital, podría incrementar los riesgos asociados a una configuración, actualización, soporte o intervención inadecuada sobre las soluciones actualmente implementadas.

El nivel Expert constituye un elemento diferenciador frente a una membresía básica, pues Fortinet lo reserva para partners que han demostrado capacidades para entregar el espectro de sus soluciones y cuentan con personal altamente capacitado y certificado para gestionar implementaciones de mayor complejidad. En consecuencia, este nivel permite a la Entidad contar con un integrador cuya relación con el fabricante no se limita a la comercialización de productos, sino que se encuentra respaldada por conocimiento especializado, capacidades técnicas internas y experiencia demostrable en el despliegue y soporte de tecnologías Fortinet.

Para una institución como el HOSPITAL MILITAR CENTRAL, donde la continuidad, confidencialidad, integridad y disponibilidad de la información resultan especialmente relevantes, consideramos necesario elevar el nivel de aseguramiento técnico del futuro contratista. La participación de un Partner Expert, acompañada de personal certificado y experiencia acreditada en proyectos Fortinet, contribuye a disminuir los riesgos de ejecución y brinda mayores garantías frente al diagnóstico, configuración, actualización, soporte y escalamiento de situaciones que puedan presentarse durante la ejecución contractual.

Por lo anterior, solicitamos respetuosamente que se requiera al oferente acreditar mediante certificación o comunicación expedida directamente por Fortinet su condición vigente de Partner nivel Expert.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

El requisito de acreditación como Partner autorizado de Fortinet fue establecido con el propósito de verificar que el oferente cuente con una relación vigente y reconocida por el fabricante para la comercialización, implementación y soporte de las soluciones objeto del proceso. La exigencia de un nivel específico dentro del programa de canales, como Expert, no resulta necesaria para acreditar por sí sola la capacidad técnica requerida para la ejecución contractual.

La idoneidad del futuro contratista será verificada de manera integral a través de los requisitos establecidos en el proceso, incluyendo la acreditación como partner autorizado, la experiencia exigida y las competencias del personal técnico requerido. En este sentido, elevar la condición mínima a un nivel específico del programa comercial del fabricante restringiría la participación sin que ello represente, por sí mismo, una garantía adicional indispensable frente al cumplimiento de las obligaciones técnicas previstas.

Por lo anterior, se mantiene el requisito de acreditar la condición de Partner autorizado de Fortinet, sin exigir específicamente el nivel Expert.

OBSERVACIONES FORMULADAS POR COMPAÑÍA DE INGENIEROS DE SISTEMAS ASOCIADOS COINSA SAS.

OBSERVACIÓN No. 1

OBSERVACIÓN No. 1 – SOLICITUD DE NIVEL EXPERT DEL FABRICANTE FORTINET

De acuerdo con los requerimientos establecidos en el Anexo Técnico y considerando que dentro del proceso se solicita acreditar mediante carta la calidad de Partner del fabricante Fortinet, respetuosamente solicitamos a la Entidad considerar que dicha acreditación corresponda al máximo nivel de membresía vigente dentro del programa de canales del fabricante, esto es, nivel Expert, o la denominación equivalente que Fortinet establezca para dicho nivel al momento de la presentación de la oferta.

La presente solicitud encuentra sustento técnico en la naturaleza, criticidad y alcance de la infraestructura objeto del proceso. No se trata únicamente del suministro o renovación de licenciamiento, sino de garantizar la actualización, soporte y adecuada continuidad de una plataforma de ciberseguridad que hace parte de la infraestructura tecnológica del Hospital Militar Central, entidad que por su naturaleza presta servicios esenciales de salud y atiende población vinculada al Sector Defensa. El propio objeto contractual comprende la adquisición de la suscripción, actualización del licenciamiento y soporte de la solución Fortinet actualmente implementada en el Hospital.

En este contexto, consideramos que el nivel de relacionamiento y especialización del contratista frente al fabricante constituye un elemento técnico relevante para disminuir los riesgos asociados con la ejecución. Fortinet define a sus partners Expert como organizaciones que han demostrado experiencia en la entrega del espectro de soluciones del fabricante y que disponen de personal altamente entrenado y certificado para gestionar implementaciones de mayor complejidad.

Una infraestructura de seguridad de estas características requiere capacidades que trascienden la comercialización de licencias: conocimiento profundo de arquitectura, configuración, interoperabilidad, actualización, soporte, diagnóstico y escalamiento, así como capacidad para atender oportunamente incidentes o situaciones que puedan comprometer la disponibilidad y seguridad de los servicios tecnológicos de la Entidad.

Lo anterior adquiere especial relevancia teniendo en cuenta que el mismo pliego exige que el contratista ejecute idónea y eficazmente el objeto contractual, mantenga niveles de eficiencia técnica y ejerza permanentemente autocontrol sobre las actividades, procesos y productos asociados al contrato. Asimismo, establece obligaciones de reserva

sobre la información técnica y las instalaciones del Hospital, evidenciando el carácter sensible de la infraestructura involucrada.

Por lo anterior, respetuosamente solicitamos al Hospital Militar Central modificar el requisito correspondiente a la carta de Partner, estableciendo que el proponente deberá acreditar mediante certificación o carta expedida directamente por Fortinet su condición vigente de Partner nivel Expert, o su denominación equivalente vigente, con el propósito de garantizar que el futuro contratista cuente con el máximo nivel de relacionamiento, capacidad técnica, especialización y respaldo del fabricante requerido para la adecuada ejecución del objeto contractual.

Consideramos que esta condición fortalece técnicamente el proceso, reduce los riesgos de ejecución y brinda a la Entidad un mayor nivel de respaldo frente a una plataforma directamente relacionada con la protección y continuidad de su infraestructura tecnológica.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

La acreditación como Partner autorizado de Fortinet tiene como finalidad verificar que el oferente mantiene una relación vigente y reconocida por el fabricante para la comercialización, implementación y soporte de las soluciones objeto del proceso. Sin embargo, no se considera necesario exigir que dicha condición corresponda específicamente al nivel Expert o al máximo nivel vigente dentro del programa de canales.

La capacidad técnica requerida para la correcta ejecución del contrato no se determina únicamente por el nivel de membresía comercial del oferente frente al fabricante. Esta se verifica de manera integral mediante los requisitos técnicos, la experiencia exigida, las certificaciones del personal asignado y las demás condiciones establecidas en los documentos del proceso. En consecuencia, exigir el nivel más alto del programa de partners incorporaría una condición adicional que no resulta indispensable para acreditar la idoneidad técnica necesaria para el cumplimiento del objeto contractual.

Por lo anterior, se mantiene el requisito de acreditar la condición vigente de Partner autorizado de Fortinet, sin exigir específicamente el nivel Expert ni el máximo nivel de membresía del programa de canales del fabricante.

OBSERVACIÓN No. 2

OBSERVACIÓN No. 2 – FACTOR PONDERABLE DE ANÁLISIS DE VULNERABILIDADES – SOLICITUD DE PRESTACIÓN MEDIANTE SOC PROPIO CERTIFICADO

Respecto del factor ponderable mediante el cual se asignan 100 puntos al oferente que, sin costo adicional, realice trimestralmente análisis de vulnerabilidades, análisis de riesgos y pruebas integrales sobre los activos de información definidos por la Entidad, entregando los respectivos informes y orientación para su corrección, respetuosamente solicitamos fortalecer las condiciones bajo las cuales deberá prestarse este servicio.

Si bien diferentes herramientas tecnológicas permiten ejecutar análisis automatizados de vulnerabilidades, consideramos que el verdadero valor agregado para el Hospital Militar Central no se encuentra exclusivamente en la ejecución de un escaneo o en la generación periódica de un informe, sino en la capacidad especializada existente detrás del servicio para analizar, correlacionar, priorizar y gestionar técnicamente los hallazgos identificados.

Por lo anterior, solicitamos que para la obtención de los 100 puntos correspondientes a este factor, el servicio sea prestado directamente a través de un Centro de Operaciones

de Seguridad – SOC propio del oferente, respaldado por capacidades especializadas de respuesta a incidentes, y que dicho SOC se encuentre cubierto por una certificación vigente ISO/IEC 27001:2022 y cuente con un equipo de respuesta a incidentes que sea miembro pleno de FIRST (Forum of Incident Response and Security Teams).

La operación mediante un SOC propio permite que los resultados del análisis de vulnerabilidades sean gestionados dentro de una capacidad operacional permanente de ciberseguridad y no como una actividad aislada. Esto permite incorporar especialistas, procedimientos definidos, trazabilidad, priorización basada en riesgo, análisis del contexto de las vulnerabilidades, identificación de amenazas relacionadas y acompañamiento técnico para establecer medidas de remediación. En una infraestructura de la criticidad del Hospital Militar Central, estas capacidades proporcionan un mayor valor técnico al ejercicio periódico solicitado por la Entidad.

Asimismo, consideramos pertinente que el SOC se encuentre cubierto por una certificación ISO/IEC 27001:2022 vigente. Esta norma internacional establece los requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información y proporciona un marco sistemático para gestionar los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información. ISO Por consiguiente, la certificación permite acreditar que el servicio se desarrolla dentro de un sistema formal de gestión de seguridad de la información y bajo controles y procesos verificables.

De manera complementaria, solicitamos que el oferente acredite que el equipo SOC es miembro pleno de FIRST. FIRST es el foro global que reúne equipos especializados de respuesta a incidentes de seguridad y promueve la cooperación, coordinación, prevención, reacción ante incidentes e intercambio de información entre sus miembros. La organización cuenta actualmente con una comunidad internacional de más de 800 equipos. FIRST Forum

La pertenencia como equipo miembro de FIRST resulta especialmente relevante porque su proceso de admisión contempla patrocinio por miembros existentes y la evaluación de capacidades operacionales del equipo; dentro de los aspectos considerados por FIRST se encuentran procesos de prevención, detección, resolución y manejo de incidentes, así como mecanismos de auditoría y retroalimentación. Por tanto, no se trataría únicamente de acreditar la existencia nominal de un SOC, sino de demostrar capacidades organizacionales y operacionales especializadas para gestionar eventos e incidentes de ciberseguridad.

Para el Hospital Militar Central, la combinación de un SOC propio, un Sistema de Gestión de Seguridad de la Información certificado bajo ISO/IEC 27001:2022 y un CSIRT/CERT miembro pleno de FIRST proporciona elementos objetivos para diferenciar una oferta que simplemente incorpora una herramienta de análisis de vulnerabilidades de aquella que ofrece una capacidad especializada y estructurada para gestionar el riesgo asociado a los hallazgos encontrados.

Por lo anterior, respetuosamente solicitamos a la Entidad modificar el factor ponderable estableciendo que los 100 puntos sean otorgados al oferente que se comprometa a realizar, sin costo adicional, los análisis trimestrales establecidos mediante un SOC propio, cuyo alcance se encuentre cubierto por certificación ISO/IEC 27001:2022 vigente y que cuente como miembro pleno de FIRST, acreditando dichas condiciones mediante los certificados o documentos correspondientes.

Consideramos que esta modificación mantiene la finalidad originalmente prevista por la Entidad, pero fortalece sustancialmente el valor agregado recibido, incorporando capacidades verificables de gestión, análisis y respuesta en ciberseguridad acordes con la naturaleza y criticidad de la infraestructura tecnológica del Hospital Militar Central.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

El factor ponderable fue definido para valorar un servicio adicional concreto, consistente en la realización trimestral de análisis de vulnerabilidades, análisis de riesgos y pruebas integrales sobre los activos de información definidos por el Hospital, junto con la entrega de los respectivos informes y la orientación para la corrección de los hallazgos identificados. La condición evaluada corresponde al resultado y alcance del servicio ofrecido, y no a la obligación de que este sea prestado exclusivamente mediante una determinada estructura organizacional del oferente.

En este sentido, exigir que el servicio sea ejecutado únicamente a través de un SOC propio, que además se encuentre cubierto por certificación ISO/IEC 27001:2022 y cuente con un equipo miembro pleno de FIRST, incorporaría condiciones adicionales que exceden lo necesario para verificar el cumplimiento del servicio que se pretende valorar. El criterio ponderable está orientado a la ejecución de los análisis, la identificación y priorización de hallazgos, la entrega de informes y la orientación para su corrección efectiva, por lo que no se considera procedente adicionar exigencias organizacionales o acreditaciones que no resultan indispensables para alcanzar dicha finalidad técnica.

Por lo anterior, se mantiene el factor ponderable en los términos definidos, otorgando los 100 puntos al oferente que se comprometa, sin costo adicional, a realizar trimestralmente los análisis de vulnerabilidades, análisis de riesgos y pruebas integrales requeridas, entregar los informes correspondientes y brindar la orientación necesaria para su corrección efectiva.

OBSERVACIÓN No. 3

OBSERVACIÓN No. 3 Referente al ítem 4.1. CARACTERÍSTICAS Y ESPECIFICACIONES TÉCNICAS ESENCIALES

Validando en el portal de fábrica, se encuentra FortiMail Cloud (FEVMCLM000230969) el estado del soporte es vencido, Se solicita amablemente a la entidad confirmar si esta solución de FortiMail Cloud va a hacer parte de la renovación ya que no se observa dentro del requerimiento.

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que, para efectos del presente proceso, únicamente serán objeto de renovación los licenciamientos y soluciones expresamente relacionados en el numeral 4.1 "Características y Especificaciones Técnicas Esenciales" del Estudio Previo de la Licitación LP-007-2026.

OBSERVACIÓN No. 4

OBSERVACIÓN No. 4 Se solicita amablemente a la entidad confirmar la cantidad de activos que serán objeto del análisis de vulnerabilidades (direcciones IP, hosts, aplicaciones web, dominios o subdominios, según aplique), con el fin de permitir la verificación y el cumplimiento del alcance durante la ejecución del servicio.

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que, para efectos del presente proceso se realizarán análisis de vulnerabilidades alrededor de 2 dominios, unos 30 servidores, 100 hosts y 6 aplicaciones web.

OBSERVACIÓN No. 5

OBSERVACION No. 5: IDIOMA

En relación con los documentos establecidos en idioma distinto al castellano, actualmente, se requiere que los proponentes presenten traducción oficial al castellano:

1.6.IDIOMA

Los documentos y las comunicaciones entregadas, enviadas o expedidas por el Proponente o por terceros para efectos del Proceso de Contratación, o para ser tenidos en cuenta en el mismo, deben ser otorgados en castellano. La Oferta y sus anexos deben ser presentados en castellano. Los documentos en los cuales el Proponente acredite los requisitos habilitantes de que estén en una lengua extranjera, deben ser presentados en su lengua original junto con la traducción oficial al castellano. El proponente puede presentar con la oferta documentos con una traducción simple al castellano y entregar la traducción oficial al castellano dentro del plazo previsto para la subsanación. La traducción oficial debe ser el mismo texto presentado.

Solicitamos amablemente a la entidad permitir que los proponentes presenten documentación técnica en traducción simple, esto según la CIRCULAR ÚNICA EXTERNA emitida por Colombia Compra Eficiente en donde indica: “En el caso de documentos especializados, como, por ejemplo, especificaciones o fichas técnicas, que en el mercado sean de amplia utilización y aceptación en idioma distinto al castellano, las Entidades Estatales podrán establecer en los Documentos del Proceso la posibilidad de que sean aportados en su lengua original acompañados de una traducción simple al castellano”

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que se acoge la observación.

Se aclara que, de conformidad con lo establecido en el numeral 1.6 “Idioma”, los documentos presentados en lengua extranjera podrán aportarse en su idioma original acompañados de traducción simple al castellano, incluyendo fichas técnicas, datasheets, manuales, certificaciones técnicas y certificaciones del personal. En los casos en que corresponda y sea requerido por el comité, la traducción oficial al castellano podrá ser presentada dentro del plazo previsto para la subsanación, conforme a las condiciones ya establecidas en el numeral citado.

OBSERVACIONES FORMULADAS POR DATAPULSE-SECURITY SAS.

OBSERVACIÓN No. 1

Respetuosamente solicitamos a la Entidad ampliar el requisito de experiencia establecido, permitiendo acreditar contratos cuyo objeto y/o actividades contractuales estén relacionados con la **actualización y/o renovación y/o suministro de licenciamiento de plataformas de seguridad o ciberseguridad.**

Lo anterior, teniendo en cuenta que este tipo de contratos guarda relación directa con el alcance requerido y permite acreditar experiencia técnica pertinente en la provisión, renovación y gestión de soluciones de seguridad informática, sin restringir la experiencia a una marca o fabricante específico.

En este sentido, sugerimos ajustar el numeral así:

“El objeto contractual y/o las actividades contractuales deberán acreditar la actualización y/o renovación y/o suministro de licenciamiento de plataformas de seguridad o ciberseguridad.”

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que se acoge la observación.

Revisado el requisito de experiencia, se considera técnicamente procedente ampliar su alcance para permitir la acreditación de contratos relacionados con **la actualización, renovación y/o suministro de licenciamiento de plataformas de seguridad o ciberseguridad, teniendo en cuenta que estas actividades guardan relación directa con la naturaleza del objeto contractual y permiten verificar experiencia pertinente en la ejecución de este tipo de soluciones.**

El Comité considera que esta experiencia resulta suficiente y pertinente para acreditar la capacidad requerida, en la medida en que corresponde al alcance técnico que se pretende verificar dentro del presente proceso. Por tanto, no resulta necesario restringir la experiencia a una solución o fabricante específico para efectos de acreditar este requisito.

Por lo anterior, se realizará el ajuste correspondiente al requisito de experiencia, el cual quedará así:

“El objeto contractual y/o las actividades contractuales deberán acreditar la actualización y/o renovación y/o suministro de licenciamiento de plataformas de seguridad o ciberseguridad.”

OBSERVACIONES FORMULADAS POR NFRA NUBE DIGITAL S.A.S.

OBSERVACIÓN No. 1

Observación #1

Frente al numeral 4.1 “Características y especificaciones técnicas esenciales”, específicamente en el apartado de “Requerimientos Adicionales – Soporte del Fabricante”, se solicita aclarar el alcance del soporte requerido, teniendo en cuenta que allí se indica que el oferente deberá contemplar soporte 7x24 del fabricante Fortinet para la atención de casos de soporte sobre los productos licenciados.

No obstante, en el numeral 6.11 “Proyección precio techo, cantidades a adquirir y presupuesto oficial”, dentro de la descripción de los ítems objeto de renovación, se hace referencia a licenciamientos FortiCare bajo modalidad 8x5 para algunos de los productos relacionados. Esta diferencia genera ambigüedad frente al tipo de soporte de fábrica que deberá ser tenido en cuenta para la estructuración de la oferta técnica y económica.

En ese sentido, se solicita aclarar si el soporte de fábrica exigido para los productos licenciados deberá ser 7x24, conforme a lo señalado en el numeral 4.1, o si deberá mantenerse el soporte 8x5 indicado en las descripciones de los ítems del numeral 6.11. Así mismo, se solicita precisar cuál será el alcance del soporte que deberá prestar directamente el contratista, diferenciándolo del soporte emitido por el fabricante, con el fin de establecer claramente las obligaciones aplicables a cada parte.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que se acoge la observación.

Revisados los numerales señalados, se aclara que el soporte técnico 7x24 corresponde a la obligación directa del contratista, quien deberá garantizar durante la vigencia del

licenciamiento la atención especializada, gestión de incidentes, escalamiento de casos, soporte remoto y, cuando se requiera, desplazamiento a sitio dentro de los tiempos establecidos en los documentos del proceso.

Por su parte, el soporte del fabricante Fortinet corresponderá a la modalidad de licenciamiento adquirido, el cual se encuentra igualmente reflejado en el numeral 4.1 ítem 1 "ACTUALIZACIÓN DEL LICENCIAMIENTO Y SOPORTE DE LA SOLUCIÓN FORTINET", donde se relacionan las cantidades requeridas y las condiciones de soporte asociadas a los licenciamientos que permiten cubrir el 100 % de la necesidad definida para el proceso.

Se realizará el ajuste correspondiente en el apartado "Soporte del Fabricante", reemplazando la referencia a soporte 7x24 por soporte según el tipo de licenciamiento renovado del fabricante Fortinet, manteniéndose el servicio 7x24 a cargo del contratista en los términos establecidos en las obligaciones específicas del proceso.

OBSERVACIÓN No. 2

Observación #2

Frente al numeral 10 "Requisitos Técnicos Habilitantes – Personal Requerido", se solicita respetuosamente a la Entidad revisar y fortalecer las condiciones exigidas para los ingenieros certificados que estarán a cargo de la ejecución del proyecto, incorporando dentro del requisito formación de posgrado en seguridad de redes, seguridad informática, ciberseguridad o áreas afines.

Lo anterior, teniendo en cuenta que el alcance del proceso no se limita a la renovación de licenciamiento, sino que incluye soporte, actualizaciones, atención de casos, acompañamiento técnico y continuidad operativa de una solución de seguridad Fortinet para el Hospital Militar Central. Esta solución involucra componentes asociados a FortiGate, FortiAnalyzer, FortiWeb, Forti XDR, FortiPhish/FortiSAT, FortiClient EMS Cloud y FortiNAC, así como funcionalidades de protección, control, análisis, monitoreo, respuesta y administración de seguridad.

Adicionalmente, dentro de las obligaciones previstas para el contratista se establece la elaboración y entrega de un análisis integral de seguridad informática de la infraestructura objeto del contrato, en el cual se evidencie el estado actual de la solución de seguridad del Hospital Militar Central, se identifiquen vulnerabilidades, riesgos, configuraciones susceptibles de mejora y demás aspectos relevantes, formulando un plan de mejora con recomendaciones técnicas priorizadas. Dicho análisis, además, debe ser elaborado y suscrito por un profesional en Ingeniería de Sistemas o afines, con especialización en Seguridad Informática o áreas relacionadas.

Bajo ese contexto, resulta coherente que los ingenieros vinculados por el oferente acrediten no solo certificaciones técnicas de fabricante, sino también formación especializada en seguridad de redes, seguridad informática o ciberseguridad, que les permita contar con criterios técnicos para apoyar actividades de diagnóstico, análisis de riesgos, identificación de vulnerabilidades, revisión de configuraciones, formulación de recomendaciones y soporte seguro de la infraestructura.

Se solicita ajustar el requisito de personal requerido, de manera que los dos (2) ingenieros certificados vinculados por el oferente acrediten, además de las certificaciones técnicas Fortinet ya exigidas, formación de posgrado en seguridad de redes, seguridad informática, ciberseguridad o áreas afines.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que se acoge la observación.

Revisado el numeral 10 "Requisitos Técnicos Habilitantes – Personal Requerido" y su relación con las obligaciones específicas establecidas para la ejecución del contrato, se

considera técnicamente procedente complementar la formación exigida a los dos (2) ingenieros certificados vinculados por el oferente.

Lo anterior obedece a que las actividades previstas no se limitan a la atención operativa o al soporte de las soluciones Fortinet. Dentro del alcance contractual se contemplan actividades de actualización, soporte, atención de casos, revisión de configuraciones, continuidad operativa y, adicionalmente, la elaboración de un análisis integral de seguridad informática de la infraestructura objeto del contrato, en el cual deberán identificarse vulnerabilidades, riesgos, configuraciones susceptibles de mejora y formularse recomendaciones técnicas priorizadas.

En este contexto, las certificaciones técnicas de fabricante permiten acreditar conocimiento específico sobre las plataformas y productos Fortinet, mientras que la formación de posgrado en Seguridad de Redes, Seguridad Informática, Ciberseguridad o áreas afines complementa dichas capacidades con criterios de análisis, gestión de riesgos, seguridad de infraestructura y evaluación de controles, necesarios para las actividades previstas durante la ejecución.

Por lo anterior, se realizará el ajuste correspondiente al requisito de personal siendo modificado de la siguiente manera:

PERSONAL REQUERIDO

Contar con mínimo dos (2) ingenieros certificados vinculados por el oferente en donde se pueda establecer que cada uno cuenta con formación de posgrado en Seguridad de Redes o Seguridad Informática o Ciberseguridad y mínimo cuatro (04) de las siguientes certificaciones NSE3, NSE4, NSE5, NSE6 y NSE7 (o su equivalente a la fecha) de los productos FORTINET, para lo cual deberá adjuntar las hojas de vida y los certificados correspondientes de las personas que se encargaran de la ejecución del proyecto y que permita a la entidad verificar la idoneidad y capacidad del oferente y del personal.

OBSERVACIÓN No. 3

Observación #3

Frente al numeral 4.1. Características y especificaciones técnicas esenciales Requerimientos Adicionales, se solicita amablemente a la Entidad aclarar cuáles soportes deberán ser presentados por el oferente junto con la propuesta y cuáles actividades corresponderán al contratista durante la ejecución contractual.

Lo anterior, teniendo en cuenta que dentro del alcance se mencionan actividades las cuales dependen de la adjudicación del contrato, la activación de los servicios y la coordinación previa con la Entidad.

Así mismo, se solicita precisar si con la oferta deberá aportarse algún documento específico que acredite la disponibilidad de mesa de ayuda, centro de atención, canal de soporte, procedimiento de atención de casos o certificación equivalente, o si estas condiciones serán verificadas únicamente durante la ejecución del contrato.

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que las actividades relacionadas con la prestación del soporte técnico, atención y escalamiento de casos, mantenimiento preventivo, registro de licencias, elaboración del análisis integral de seguridad, transferencia de conocimiento y demás actividades operativas previstas en los requerimientos adicionales corresponden a obligaciones que deberán ser ejecutadas por el contratista durante la vigencia contractual, conforme a las condiciones y tiempos establecidos en los documentos del proceso.

No obstante, con la presentación de la oferta el proponente deberá aportar la documentación que permita acreditar previamente la disponibilidad y organización del servicio de soporte, para lo cual deberá anexar:

- El procedimiento o documento en el que se describa la forma y modalidad de atención, incluyendo mecanismos de contacto, registro, escalamiento y seguimiento de casos.

- Certificación expedida por la mesa de ayuda o centro de atención correspondiente, mediante la cual se acredite que el oferente cuenta con dicho servicio.

La ejecución material de las actividades de soporte y demás obligaciones operativas corresponderá al contratista durante la ejecución contractual, mientras que los documentos anteriormente señalados deberán ser acreditados junto con la oferta.

OBSERVACIÓN No. 4

Observación #4

Teniendo en cuenta que la solución cuenta con herramientas de administración, monitoreo y soporte remoto que permiten realizar actividades de diagnóstico, revisión y seguimiento sin requerir necesariamente desplazamiento a sitio, solicitamos a la Entidad modificar el requerimiento de cuatro (4) visitas presenciales de mantenimiento preventivo, permitiendo que se contemplen mínimo dos (2) visitas presenciales y que las demás actividades puedan ser ejecutadas de manera remota, de acuerdo con las necesidades identificadas durante la ejecución contractual.

Lo anterior permitiría optimizar los recursos asociados a la prestación del servicio sin afectar las condiciones de soporte, mantenimiento y continuidad requeridas.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

Las cuatro (4) visitas técnicas presenciales hacen parte del mantenimiento preventivo programado durante la vigencia y tienen como finalidad permitir la intervención directa sobre los equipos objeto del contrato, de acuerdo con las actividades, equipos y fechas previamente definidas en el cronograma que deberá presentar el contratista.

Si bien determinadas actividades de monitoreo, diagnóstico o soporte pueden realizarse de manera remota, estas no sustituyen el alcance de las visitas presenciales previstas, toda vez que cada una deberá generar el correspondiente informe técnico con las actividades realizadas, hallazgos, recomendaciones y acciones de mejora.

Se mantiene la exigencia de mínimo cuatro (4) visitas técnicas presenciales durante la vigencia del licenciamiento, sin perjuicio del uso complementario de herramientas de soporte o administración remota.

OBSERVACIÓN No. 5

Observación #5

Solicitamos a la Entidad permitir que la transferencia de conocimiento de treinta y dos (32) horas pueda desarrollarse en modalidad presencial, virtual sincrónica o híbrida, garantizando en todos los casos la interacción directa con el instructor, el desarrollo del contenido requerido y la participación del personal designado por la Entidad.

Consideramos que permitir diferentes modalidades de ejecución no disminuye el alcance técnico de la actividad y facilita la disponibilidad de profesionales especializados para su desarrollo.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

La transferencia de conocimiento de treinta y dos (32) horas corresponde a una obligación a cargo del contratista durante la ejecución contractual y fue definida en modalidad presencial con el propósito de garantizar una interacción directa con el personal designado por el Hospital, así como el desarrollo práctico de los contenidos asociados a la solución Fortinet desplegada.

El Comité considera necesario mantener la modalidad presencial, teniendo en cuenta que la actividad busca no solo exponer contenidos, sino facilitar la revisión directa de la solución implementada, resolver inquietudes sobre su operación y administración y fortalecer el conocimiento del personal que tendrá relación con la plataforma durante su funcionamiento.

Se mantiene la exigencia de realizar la transferencia de conocimiento en modalidad presencial, con una intensidad mínima de treinta y dos (32) horas, en los términos establecidos en los documentos del proceso.

OBSERVACIÓN No. 6

Observación #6

Frente al numeral 4.3 "Obligaciones específicas del contratista", punto 8, se solicita aclarar el alcance del análisis integral de seguridad informática requerido para la infraestructura objeto del contrato.

Teniendo en cuenta que el requisito indica que dicho análisis deberá evidenciar el estado actual de la solución de seguridad del Hospital Militar Central, identificar vulnerabilidades, riesgos, configuraciones susceptibles de mejora y formular un plan de mejora con recomendaciones técnicas priorizadas. No obstante, no se precisa si el análisis deberá limitarse únicamente a los productos y licenciamientos Fortinet objeto de renovación, o si deberá incluir otros componentes de la infraestructura tecnológica del Hospital que no hacen parte directa del alcance contractual.

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que el análisis previsto en el numeral 4.3, punto 8, se encuentra limitado a la revisión técnica de las soluciones, equipos, licenciamientos y componentes Fortinet objeto del presente contrato, y no corresponde a un análisis general de toda la infraestructura tecnológica del Hospital Militar Central.

Para efectos de esta obligación, el análisis estará orientado principalmente a verificar el estado de la solución contratada y podrá contemplar, entre otros, los siguientes aspectos:

- estado general de los equipos, licenciamientos y servicios objeto de renovación;
- revisión de versiones de software o firmware y actualizaciones aplicables a los componentes objeto del contrato;
- revisión general de configuraciones relevantes para la operación y seguridad de la solución;
- identificación de configuraciones susceptibles de mejora;
- revisión de alertas, eventos o información disponible en las plataformas objeto del contrato;
- formulación de recomendaciones técnicas y acciones de mejora relacionadas con la solución Fortinet.

Como resultado, el contratista deberá presentar un informe con los principales hallazgos identificados y las recomendaciones correspondientes.

OBSERVACIONES FORMULADAS POR XOREX DE COLOMBIA SAS.

OBSERVACIÓN No. 1

La entidad menciona en los requisitos habilitantes lo siguiente:

2	PERSONAL REQUERIDO Contar con mínimo dos (2) ingenieros certificados vinculados por el oferente en donde se pueda establecer que cada uno cuenta con mínimo cuatro (04) de las siguientes certificaciones NSE3, NSE4, NSE5, NSE6 y NSE7 (o su equivalente a la fecha) de los productos FORTINET, para lo cual deberá adjuntar las hojas de vida y los certificados correspondientes de las personas que se encargaran de la ejecución del proyecto y que permita a la entidad verificar la idoneidad y capacidad del oferente y del personal.
---	--

Respetuosamente, solicitamos a la Entidad revisar y modificar el requisito relacionado con la cantidad de ingenieros certificados exigidos al oferente, considerando que la exigencia de un número determinado de profesionales podría limitar la pluralidad de oferentes y la participación de empresas que cuentan con la capacidad técnica, experiencia e idoneidad necesarias para ejecutar adecuadamente el objeto contractual. En este sentido, consideramos que la exigencia puede ser atendida de manera suficiente mediante la disponibilidad de un profesional certificado que respalde técnicamente la solución ofertada, sin que sea necesario establecer un número superior de ingenieros que pueda generar una barrera de participación.

Por lo anterior, solicitamos amablemente a la Entidad modificar el requisito, de manera que quede establecido de la siguiente forma:

“Contar con mínimo un (1) ingeniero certificado vinculado por el oferente...”

Consideramos que esta modificación permite garantizar la idoneidad y capacidad técnica requerida para la correcta ejecución del contrato, al tiempo que favorece los principios de pluralidad de oferentes, libre concurrencia, selección objetiva y participación efectiva dentro del proceso de contratación.

Agradecemos a la Entidad considerar favorablemente la presente observación y realizar el ajuste correspondiente en los documentos definitivos del proceso.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

La exigencia de contar con mínimo dos (2) ingenieros certificados responde a la necesidad de garantizar disponibilidad y continuidad técnica durante la ejecución del contrato, teniendo en cuenta que las actividades previstas comprenden renovación, actualización, soporte, atención y escalamiento de casos, mantenimiento, revisión de configuraciones y acompañamiento técnico sobre los diferentes componentes de la solución Fortinet objeto del proceso.

Adicionalmente, dentro de las obligaciones contractuales se contempla la realización de un análisis técnico de la solución, orientado a revisar el estado general de los equipos, licenciamientos y componentes objeto de renovación, verificar versiones y actualizaciones aplicables, revisar configuraciones relevantes para la operación y seguridad, identificar aspectos susceptibles de mejora y formular las recomendaciones técnicas correspondientes. Estas actividades requieren disponibilidad suficiente de personal técnico durante la ejecución.

Contar con dos profesionales permite distribuir adecuadamente las actividades, mantener capacidad de atención ante requerimientos concurrentes y reducir la dependencia operativa de un único recurso.

El Comité considera que reducir el requisito a un (1) solo ingeniero no resulta adecuado frente al alcance técnico y las necesidades de soporte previstas para la solución. Se mantiene la exigencia de mínimo dos (2) ingenieros certificados en los términos establecidos en los documentos del proceso.

OBSERVACIONES FORMULADAS POR NEXORA TECH.

OBSERVACIÓN No. 1

1. Fortalecimiento del personal técnico requerido

La ejecución del servicio no se limita a la renovación de licencias, sino que comprende la operación, soporte, atención de casos, escalamiento y acompañamiento técnico sobre una solución de seguridad que integra diferentes componentes de protección, control, análisis y administración.

Por esta razón, se considera conveniente que el personal asignado no solo acredite certificaciones asociadas a productos Fortinet, sino también conocimientos complementarios en ciberseguridad y seguridad de redes, que permitan atender de manera adecuada eventos, incidentes, diagnósticos, configuraciones, recomendaciones y actividades de soporte durante la vigencia del contrato.

En ese sentido, se solicita a la Entidad considerar que, junto con las certificaciones NSE exigidas, se acepten o valoren certificaciones complementarias relacionadas con seguridad de redes, ciberseguridad, análisis de amenazas, gestión de incidentes, pruebas de seguridad, seguridad perimetral o administración segura de infraestructura, tales como CompTIA Security+, CySA+, PenTest+, CEH, certificaciones profesionales en ciberseguridad, certificaciones en seguridad de redes o equivalentes.

Lo anterior permitiría fortalecer la capacidad técnica del equipo encargado de la ejecución, combinando el conocimiento propio de la tecnología Fortinet con competencias transversales necesarias para la operación segura, el análisis de eventos, la atención de incidentes y la continuidad de la plataforma.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que se acoge parcialmente la observación.

La ejecución del contrato contempla actividades que requieren conocimiento especializado sobre la plataforma Fortinet, pero también capacidades técnicas transversales en materia de ciberseguridad. Dentro de las obligaciones previstas se encuentran la atención y escalamiento de incidentes, revisión de configuraciones, mantenimiento, validación de condiciones de seguridad, análisis técnico de la solución, identificación de aspectos susceptibles de mejora y formulación de recomendaciones orientadas a reducir riesgos sobre la infraestructura objeto del contrato.

Las certificaciones Fortinet permiten acreditar dominio técnico sobre la operación, configuración y soporte de los productos del fabricante; sin embargo, se considera pertinente complementar dichas competencias con una certificación que permita acreditar conocimientos independientes del fabricante en fundamentos de ciberseguridad, identificación de vulnerabilidades, gestión de riesgos, respuesta ante incidentes y evaluación de condiciones de seguridad.

Analizadas las certificaciones propuestas, el Comité considera procedente incorporar como requisito adicional la acreditación de certificaciones expedidas por CompTIA, o de EC-Council organismo de certificación reconocido internacionalmente en el ámbito de tecnologías de la información y ciberseguridad. Ya que les permite acreditar conocimientos transversales en seguridad de redes, amenazas, vulnerabilidades, controles y gestión de incidentes, identificación y evaluación de vulnerabilidades y pruebas de seguridad.

Por lo anterior, se realizará el ajuste correspondiente para incluir parcialmente las recomendaciones.

OBSERVACIÓN No. 2

2. Acreditación de autorización como partner

Se solicita permitir que la condición de distribuidor autorizado o partner pueda acreditarse mediante certificación expedida por un distribuidor autorizado del fabricante, en la cual se identifique claramente al oferente y su relación comercial dentro del canal correspondiente.

Lo anterior, teniendo en cuenta que la acreditación de la relación comercial puede ser gestionada a través de la cadena de distribución autorizada, permitiendo validar la condición del oferente sin limitar su acreditación exclusivamente a una certificación expedida directamente por el fabricante.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

El requisito fue establecido para que la condición de distribuidor autorizado o partner sea acreditada directamente por el fabricante de la solución ofertada, con el fin de verificar de manera expresa y verificable que el oferente mantiene una relación vigente y reconocida dentro del programa de canales correspondiente.

Una certificación expedida únicamente por un distribuidor autorizado acredita una relación comercial dentro de la cadena de suministro, pero no sustituye la validación directa por parte del fabricante respecto de la condición de partner o distribuidor autorizado del oferente. Por esta razón, no se considera procedente ampliar el medio de acreditación en los términos solicitados.

Se mantiene el requisito de aportar certificación expedida por el fabricante de la solución ofertada que acredite al oferente como distribuidor autorizado o partner.

OBSERVACIÓN No. 3

3. Alcance de la licencia de simulación avanzada de ataques cibernéticos — Cyber Range

Al revisar el criterio ponderable que establece el ofrecimiento de una (1) licencia de servicio de simulación avanzada de ataques cibernéticos — Cyber Range, con una duración de ocho (8) horas, se solicita aclarar si el requerimiento corresponde únicamente a la ejecución de una jornada de ocho (8) horas para hasta doce (12) participantes, o si la licencia deberá contar con una vigencia determinada durante el plazo de ejecución del contrato.

Esta precisión resulta necesaria para determinar correctamente el alcance del ofrecimiento, la duración real del servicio, las condiciones de acceso a la plataforma y los costos asociados que deberán ser contemplados por los oferentes.

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que el requerimiento corresponde a una (1) jornada de ocho (8) horas de servicio de simulación avanzada de ataques cibernéticos — Cyber Range, para un máximo de doce (12) participantes.

no se exige una vigencia adicional de la licencia durante el plazo de ejecución del contrato. El ofrecimiento deberá contemplar el acceso a la plataforma y los recursos

necesarios para el desarrollo completo de dicha jornada, en los términos establecidos en el criterio ponderable.

OBSERVACIÓN No. 4

4. Periodicidad de la campaña de Phishing

Respecto del criterio ponderable que establece la realización de una campaña de Phishing “bimensual” durante la vigencia del licenciamiento, se solicita aclarar la periodicidad requerida, indicando si corresponde a dos (2) campañas mensuales o a una (1) campaña cada dos (2) meses.

Esta aclaración resulta necesaria para determinar correctamente la cantidad de campañas, informes, actividades de seguimiento y recursos que deberán ser contemplados durante la vigencia del licenciamiento.

Agradecemos a la Entidad revisar las observaciones presentadas y realizar las aclaraciones o ajustes que considere pertinentes, con el fin de permitir una estructuración adecuada, objetiva y comparable de las ofertas.

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que la periodicidad establecida como bimensual corresponde a la realización de una (1) campaña de Phishing cada dos (2) meses, durante la vigencia del licenciamiento.

Cada campaña deberá contemplar las actividades previstas en el criterio ponderable, incluyendo su ejecución, seguimiento y la entrega del informe correspondiente, de acuerdo con las condiciones establecidas.

OBSERVACIÓN No. 5

5. Tiempo de desplazamiento para atención presencial

Se solicita considerar la ampliación del tiempo máximo establecido para el desplazamiento de personal técnico especializado a las instalaciones del Hospital, pasando de dos (2) a cuatro (4) horas cuando se requiera atención presencial, manteniendo el tiempo máximo de respuesta telefónica definido en el documento.

RESPUESTA:

El Comité Técnico Estructurador se permite informar al observante que no se acoge la observación.

El tiempo máximo de dos (2) horas para el desplazamiento de personal técnico especializado, cuando se requiera atención presencial, fue establecido teniendo en cuenta la naturaleza de la solución y la necesidad de contar con capacidad de respuesta oportuna ante incidentes o situaciones que no puedan ser solucionadas de manera remota.

La atención telefónica y remota constituye el primer nivel de respuesta; sin embargo, cuando el diagnóstico determine la necesidad de intervención presencial, se requiere mantener un tiempo de desplazamiento que permita atender oportunamente la situación y reducir el impacto que una eventual indisponibilidad pueda generar sobre los servicios de seguridad objeto del contrato.

Por lo anterior, se mantiene el tiempo máximo de dos (2) horas para la atención presencial cuando esta sea requerida, así como las demás condiciones de soporte

establecidas en los documentos del proceso.

OBSERVACIONES FORMULADAS POR GRUPO LUMA SAS.

OBSERVACIÓN No. 1

Se solicita transferencia de conocimiento mediante capacitación dirigida a personal designado.

*Cuántas personas componen este grupo de "personas designadas"?

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que serian alrededor de 8 personas.

OBSERVACIÓN No. 2

Modalidad Presencial,

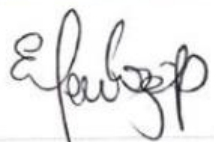
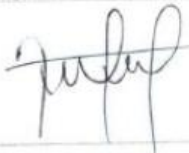
*En donde será la sede designada para la capacitación?

*Las 32 horas de capacitación serán en sesiones y temas designadas por la entidad?

RESPUESTA:

El Comité Técnico Estructurador se permite aclarar al observante que la institución cuenta con el espacio físico y los medios audiovisuales que pondrá a disposición del contratista para que lleve a cabo estas capacitaciones. Las sesiones y temáticas serán acordadas con el supervisor del contrato.

Proyectó:

DESIGNACION	NOMBRE	CARGO Y DEPENDENCIA	FIRMAS
GERENTE DE PROYECTO	Teniente Coronel Eduardo Enrique Mendoza Palacio	Jefe Unidad de Informática	
COMITÉ TÉCNICO ESTRUCTURADOR	Capitán Fernando Joya	Unidad de Informática	
COMITÉ JURÍDICO	Cristian Ramírez Medina	PS. Abogado - Área Gestión Contratos	
COMITÉ ECONÓMICO	Ramón Gómez Bueno	PD. Área Gestión Contratos	