COMANDO GENERAL
FUERZAS MILITARES DE COLOMBIA
UNIÓN - INTEGRIDAD - VICTORIA

FORMULARIO PREGUNTAS Y RESPUESTAS No. 001 AL PROYECTO DE PLIEGO DEL PROCESO DE MENOR CUANTÍA No. 126-MDN-COGFM-ESDEG-2026, CUYO OBJETO ES LA RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA PLATAFORMA DE ASEGURAMIENTO TECNOLÓGICO COMPUESTA POR LOS EQUIPOS DE SEGURIDAD PERIMETRAL Y CONECTIVIDAD FORTIGATE 600E, FORTIANALIZER 200F Y ACTUALIZACIÓN DEL EDR CON XDR (EXTENDED DETECTION AND RESPONSE), PARA LA ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"

Bogotá, D.C., 21 de julio de 2026

1. IO GESTION
26/06/2026 9:52:15 AM(UTC-05:00) Bogotá, Lima, Quito

"Buenos días Doctores, LUIS FERNANDO BECERRA VILLARRAGA, representante Legal de IOGESTION SAS, me permito solicitar respetuosamente su amable colaboración suministrándonos los seriales de las renovaciones solicitadas en el proceso, esto, toda vez, que el fabricante no nos da precios sin estos seriales"

RESPUESTA COMITÉ TECNICO: La entidad se permite informar al oferente que los seriales así:

FORTINET

Service Entitlement Summary

Date	: September 29, 2025
Sales Order #	: 1011780198
Purchase Order #	: 052842-CO
Quote ID	: 6642013-1
Co-Term Date	: September 30, 2026
Effective Date	: September 24, 2025

Registration is not required for Co-Terminus Agreements and the Entitlement Summary has been provided for Your reference. The serial numbers listed below reflect the Co-Term date requested.

FG100FTK22050829

FG6H0ETB20903177

FG6H0ETB20903052

2. HEIMCORE SAS
25/06/2026 8:32:11 PM(UTC-05:00) Bogotá, Lima, Quito

1. **PRIMERA OBSERVACION:**

Observación 1

Comedidamente solicitamos a la Entidad publicar en formato editable o texto legible los documentos correspondientes al Proceso de Selección Abreviada de Menor Cuantía No. 126-MDN-COGFM-ESDEG-2026, cuyo objeto es la Renovación de licenciamiento y soporte técnico de la plataforma de aseguramiento tecnológico compuesta por los equipos de seguridad perimetral y conectividad FortiGate 600E, FortiAnalyzer 200F y actualización del EDR con XDR (Extended Detection and Response), para la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Lo anterior, teniendo en cuenta que los documentos publicados se encuentran escaneados o en formato imagen, lo cual dificulta su consulta, búsqueda, análisis técnico y adecuada manipulación por parte de los interesados. Esta solicitud se realiza con el fin de facilitar la revisión integral de los requisitos y permitir una adecuada estructuración de las ofertas.

RESPUESTA COMITÉ JURIDICO:

Se acoge la solicitud, se publica documento en formato editable para permitir manipulación por los interesados.

SEGUNDA OBSERVACION:

Observación 2 – ESTUDIO PREVIO

ITEM 2 - RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO EDR-XDR (ADVANCED MALWARE PREVENTION DLP/APPLICATION CONTROL/DEVICE CONTROL FW/VULNERABILITY PROTECTION/WEB REPUTATION XDR)

Se solicita respetuosamente a la Entidad revisar y aclarar el alcance del Ítem 2, toda vez que en el encabezado se incluye la funcionalidad DLP y está también se refleja en los numerales 5 y 15 de las especificaciones técnicas mínimas.

Lo anterior, considerando que una solución XDR está orientada a la detección, correlación, investigación y respuesta extendida ante amenazas, mientras que una solución DLP corresponde a una herramienta especializada para la prevención de pérdida o fuga de información, con alcance, licenciamiento y dimensionamiento diferente.

Por lo anterior, se solicita aclarar si el ítem 2 requiere únicamente una solución EDR-XDR. En caso afirmativo, se solicita eliminar o ajustar las referencias a DLP en el encabezado y en los numerales 5 y 15.

En caso de que la Entidad requiera una solución DLP, se solicita crear un ítem independiente con sus especificaciones técnicas mínimas y presupuesto asociado, permitiendo a los oferentes dimensionar correctamente la solución.

RESPUESTA COMITÉ TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el alcance del Ítem 2 corresponde a la renovación/upgrade del licenciamiento y soporte técnico de una solución EDR-XDR, conforme a las necesidades técnicas definidas por la Entidad en el proceso.

La referencia a DLP incluida en el encabezado del ítem y en los numerales 5 y 15 de las especificaciones

técnicas mínimas no corresponde a la adquisición de una herramienta DLP independiente, sino a una capacidad funcional esperada dentro de la solución ofertada, orientada a la protección contra filtrado o fuga de datos sensibles, control de dispositivos y administración centralizada de políticas de seguridad.

En consecuencia, no se considera necesario crear un ítem independiente para DLP ni modificar el alcance del Ítem 2. La Entidad aceptará capacidades nativas, integradas o equivalentes que permitan cumplir el objetivo funcional requerido, sin limitar la participación a una marca o fabricante específico.

3. TERCERA OBSERVACION:

Observación 3 – ESTUDIO PREVIO

ITEM 1 RENOVACION DE LICENCIAMIENTO Y SOPORTE TECNICO FIREWALL 600E, FORTIANALYZER 300G- ITEM 1.1

Comedidamente solicitamos a la Entidad publicar o suministrar mediante mecanismo seguro la relación de seriales y fechas de vencimiento de los activos.

Lo anterior aplica para los equipos y licencias asociados a la plataforma de aseguramiento tecnológico, incluyendo FortiGate 600E, FortiAnalyzer y la solución EDR que tiene actualmente la entidad.

Esta información es necesaria para validar ante el fabricante el estado actual del licenciamiento, soporte, elegibilidad de renovación, vigencias, compatibilidad y correcta estructuración económica de la oferta.

RESPUESTA COMITÉ TECNICO:

El comité técnico se permite relacionar las fechas de caducidad del licenciamiento.

FORTINET

Service Entitlement Summary

Date	: September 29, 2025
Sales Order #	: 1011780198
Purchase Order #	: 052842-CO
Quote ID	: 6642013-1
Co-Term Date	: September 30, 2026
Effective Date	: September 24, 2025

Registration is not required for Co-Terminus Agreements and the Entitlement Summary has been provided for Your reference. The serial numbers listed below reflect the Co-Term date requested.

FG100FTK22050829

FG6H0ETB20903177

FG6H0ETB20903052

4. CUARTA OBSERVACION:

Observación 4 – Certificación del fabricante.

Comedidamente solicitamos a la Entidad incluir dentro de los requisitos técnicos habilitantes la presentación de una certificación expedida por el fabricante de la solución ofertada, en la cual conste que el proponente cuenta con membresía vigente dentro del programa oficial de canales o partners del fabricante, en alguno de sus dos (2) niveles superiores, y que se encuentra autorizado para comercializar, renovar, implementar y soportar la solución objeto del presente proceso.

Lo anterior, teniendo en cuenta que el objeto contractual corresponde a la renovación de licenciamiento y soporte técnico de una plataforma de seguridad existente, por lo cual resulta importante garantizar que el oferente cuente con respaldo directo del fabricante, conocimiento técnico, acceso a canales oficiales de soporte y capacidad para gestionar adecuadamente renovaciones, licenciamiento, garantías y atención técnica.

Así mismo, este requisito permite fortalecer la transparencia, trazabilidad y adecuada ejecución contractual, asegurando que la solución sea ofertada por canales debidamente reconocidos por el fabricante y con experiencia comprobable en las tecnologías requeridas por la Entidad.

RESPUESTA COMITÉ TECNICO:

Se acoge parcialmente la observación.

La entidad considera pertinente solicitar una certificación expedida por el fabricante de la solución ofertada, o por canal mayorista autorizado, en la cual conste que el proponente cuenta con membresía vigente dentro del programa oficial de canales o partners del fabricante y que se encuentra autorizado para comercializar, renovar, implementar y/o soportar la solución ofertada.

No obstante, con el fin de garantizar pluralidad de oferentes, no se exigirá un nivel específico de partner, siempre que el proponente acredite autorización vigente del fabricante o del canal autorizado y capacidad para gestionar el licenciamiento, soporte y renovación de la solución presentada.

Lo anterior permite garantizar respaldo del fabricante, trazabilidad en la renovación, soporte oficial y adecuada ejecución contractual, sin limitar la participación a un nivel específico dentro del programa de canales.

3. NETSECURE

25/06/2026 6:56:52 PM(UTC-05:00) Bogotá, Lima, Quito)

1. PRIMERA OBSERVACION:

OBSERVACIÓN No. 1
EXIGENCIA DE ARQUITECTURA MONOLÍTICA BASADA EN AGENTE ÚNICO
Referencia: Ítems 4, 5, 15 y 16, página 20 del documento estudio previo definitivo

Solicitamos revisar los requisitos que exigen la coexistencia de múltiples funcionalidades de seguridad dentro de un único agente endpoint.

El mercado actual de soluciones EDR/XDR ha evolucionado hacia arquitecturas distribuidas, integradas e interoperables, donde diferentes capacidades pueden ser suministradas mediante componentes especializados administrados desde una consola centralizada.

La exigencia de incorporar simultáneamente funcionalidades de Firewall, HIPS, DLP, Control de Aplicaciones y Protección de Vulnerabilidades dentro de un único agente limita la participación de arquitecturas modernas ampliamente utilizadas en el sector público y privado.

La necesidad funcional de la Entidad corresponde a la protección integral del endpoint y no a una implementación específica basada en un único componente software.

Por lo anterior, solicitamos permitir expresamente que las funcionalidades requeridas puedan ser suministradas mediante componentes nativos, integrados o interoperables administrados centralizadamente.

En atención a los requisitos técnicos establecidos en los ítems 4, 5, 15 y 16 de la página 20 del documento de estudio previo definitivo, solicitamos revisar la exigencia conforme a la cual diversas funcionalidades de seguridad, tales como Firewall, HIPS, DLP, Control de Aplicaciones y Protección de Vulnerabilidades, deben coexistir necesariamente dentro de un único agente instalado en el endpoint. La observación no pretende disminuir el alcance técnico ni el nivel de protección requerido por el proceso. Por el contrario, busca que el requisito se mantenga orientado al cumplimiento funcional de las capacidades de seguridad solicitadas, sin imponer una forma específica de implementación tecnológica que pueda limitar injustificadamente la participación de soluciones equivalentes o superiores.

En atención a los requisitos técnicos establecidos en los ítems 4, 5, 15 y 16 de la página 20 del documento de estudio previo definitivo, solicitamos revisar la exigencia conforme a la cual diversas funcionalidades de seguridad, tales como Firewall, HIPS, DLP, Control de Aplicaciones y Protección de Vulnerabilidades, deben coexistir necesariamente dentro de un único agente instalado en el endpoint. La observación no pretende disminuir el alcance técnico ni el nivel de protección requerido por el proceso. Por el contrario, busca que el requisito se mantenga orientado al cumplimiento funcional de las capacidades de seguridad solicitadas, sin imponer una forma específica de implementación tecnológica que pueda limitar injustificadamente la participación de soluciones equivalentes o superiores.

En el mercado actual de soluciones EDR/XDR, la protección integral del endpoint puede ser prestada mediante diferentes arquitecturas tecnológicas. Algunas soluciones operan mediante un agente único (*Un agente único se puede comparar con una aplicación, por ejemplo como WORD, EXCEL, POWER POINT, entre otras, lo que se pretende desde una perspectiva más entendible, es que al requerir un único agente, es como si en una sola APP se puedan tener las capacidades de WORD, EXCEL, POWER POINT, entre otras*) mientras que otras utilizan componentes nativos, módulos especializados, sensores, servicios complementarios o capacidades interoperables administradas desde una consola centralizada. Estas arquitecturas permiten cumplir los mismos objetivos de

seguridad, visibilidad, control, prevención, detección, respuesta y administración, sin que todas las funcionalidades deban residir físicamente en un único componente de software.

Bajo esa perspectiva, exigir que todas las funcionalidades mencionadas estén incorporadas en un único agente no constituye necesariamente una condición indispensable para garantizar la seguridad del endpoint, es más bien un tema de software propietario de un fabricante, de cómo elabore o desarrolle su solucion, mas no algo que afecte de manera directa el objetivo final del presente proceso.

Lo relevante para la Administración debe ser que la solución ofertada garantice el cumplimiento efectivo de las funcionalidades requeridas, la administración centralizada, la interoperabilidad entre componentes, la trazabilidad de eventos, la aplicación uniforme de políticas y la protección integral de los activos tecnológicos objeto del proceso.

La redacción actual podría restringir la pluralidad de oferentes, al privilegiar una arquitectura monolítica específica frente a otros modelos tecnológicos ampliamente utilizados en el sector público y privado, que cumplen la misma finalidad funcional.

En ese sentido, el requisito podría resultar desproporcionado frente al objeto contractual, en la medida en que condiciona la participación a una forma particular de despliegue y no exclusivamente al resultado técnico esperado.

Por lo anterior, solicitamos modificar la redacción de los ítems 4, 5, 15 y 16, con el fin de permitir que las funcionalidades requeridas puedan ser suministradas mediante un agente único o mediante componentes nativos, integrados, interoperables o módulos especializados, siempre que se encuentren administrados centralizadamente y garanticen el cumplimiento integral de las capacidades exigidas.

Se propone la siguiente redacción:

"Las funcionalidades de Firewall, HIPS, DLP, Control de Aplicaciones, Protección de Vulnerabilidades y demás capacidades de seguridad requeridas deberán ser provistas por la solución ofertada, ya sea mediante un agente único o mediante componentes nativos, integrados, interoperables o módulos especializados, siempre que sean administrados desde una consola centralizada y garanticen el cumplimiento funcional, operativo y de seguridad exigido por el proceso."

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad mantiene el requisito establecido en las especificaciones técnicas, teniendo en cuenta que la arquitectura solicitada busca garantizar una administración centralizada, menor complejidad operativa, trazabilidad unificada de eventos, aplicación homogénea de políticas de seguridad y reducción de riesgos asociados a la instalación, operación y soporte de múltiples componentes en los endpoints.

Por tal motivo, resulta necesario que la solución ofertada proporcione las capacidades requeridas de protección, control, prevención, detección y respuesta de forma integrada, asegurando continuidad operativa, facilidad de administración y una gestión eficiente de incidentes desde una consola centralizada.

En consecuencia, se mantiene el requisito en los términos establecidos en el Estudio Previo y no se modifica la especificación técnica mínima.

2. SEGUNDA OBSERVACION:

OBSERVACIÓN No. 2
OPENIOC Y YARA COMO REQUISITO OBLIGATORIO
Referencia: Página 20 - Ítem 20.

Solicitamos permitir mecanismos equivalentes para la investigación de amenazas, eliminando la exigencia específica de OpenIOC y YARA.

Lo anterior, teniendo en cuenta que la Entidad busca que la solución permita investigar incidentes de seguridad; sin embargo, OpenIOC y YARA son únicamente dos de las tecnologías existentes para cumplir ese objetivo.

Es comparable a solicitar un documento en formato PDF cuando existen otros formatos que permiten exactamente el mismo resultado. Solicitar tecnologías específicas limita la participación de fabricantes que cuentan con mecanismos propios o equivalentes para realizar investigaciones avanzadas.

RESPUESTA COMITE TECNICO:

No se acoge la observación.

El comité técnico estructurado se permite informar que se mantiene el requisito establecido en el Ítem 20, relacionado con el uso de reglas OpenIOC y YARA, teniendo en cuenta que dichas capacidades permiten fortalecer los procesos de investigación de amenazas, búsqueda de indicadores de compromiso, análisis avanzado de eventos y detección de comportamientos asociados a código malicioso.

Por lo tanto, para la ESDEG resulta necesario que la solución ofertada cuente con mecanismos avanzados y reconocidos para realizar investigaciones detalladas, programadas y bajo criterios configurables, con el fin de mejorar la capacidad de detección, análisis y respuesta frente a incidentes de seguridad.

En consecuencia, se mantiene el requisito en los términos establecidos en el Estudio Previo y no se modifica la especificación técnica mínima.

3. OBSERVACION:

OBSERVACIÓN No. 3
REPUTACIÓN DE ARCHIVOS Y URL
Referencia: Página 21 - Ítem 35.

Solicitamos permitir mecanismos equivalentes para evaluar la confiabilidad de archivos y direcciones web.

Teniendo en cuenta que cada fabricante administra sus propias bases de inteligencia de amenazas. Lo importante para la Entidad es que la solución identifique archivos o sitios maliciosos, sin importar la tecnología utilizada para lograrlo.



RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 35 hace referencia a una capacidad funcional de la solución ofertada, orientada a analizar la reputación de archivos y URL como mecanismo de apoyo para la detección, prevención y respuesta frente a amenazas.

En ese sentido, la Entidad no exige una base de datos, motor o metodología específica de un fabricante determinado, sino que la solución propuesta cuente con la capacidad de evaluar la confiabilidad o reputación de archivos y direcciones web, de acuerdo con sus propios mecanismos de inteligencia, análisis o clasificación de amenazas.

Por lo anterior, el requisito se mantiene, aclarando que podrá ser cumplido mediante las capacidades nativas o integradas de la solución EDR-XDR ofertada, siempre que permitan satisfacer el objetivo técnico requerido por la Entidad.

4. OBSERVACION:

OBSERVACIÓN No. 4
CONSOLA WEB DE ADMINISTRACIÓN
Referencia: Página 21 - ítem 34.
Solicitamos permitir cualquier mecanismo seguro de administración centralizada, teniendo en cuenta que actualmente existen fabricantes que administran sus soluciones desde consola web, aplicaciones híbridas o plataformas SaaS.

Lo relevante es garantizar la administración centralizada y segura, no la forma específica mediante la cual el fabricante implementa dicha consola.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 34, relacionado con que la consola de administración pueda ser utilizada desde un entorno web, hace referencia a la capacidad de acceso y administración mediante navegador, a través de protocolos seguros como HTTPS o equivalentes.

Por lo tanto, no está exigiendo una arquitectura específica de fabricante, ni limitando la solución a un modelo SaaS, on-premise o híbrido determinado. Lo requerido es que la solución ofertada permita la administración centralizada de la plataforma EDR-XDR mediante una interfaz web segura, que facilite la gestión de políticas, monitoreo, revisión de eventos y atención de incidentes.

En consecuencia, se mantiene el requisito en los términos establecidos, aclarando que corresponde a una funcionalidad de administración segura y no a una condición asociada a una marca, fabricante o

arquitectura particular.

5. OBSERVACION:

OBSERVACIÓN No. 5
INTEGRACIÓN EXCLUSIVA CON ACTIVE DIRECTORY
Referencia: Página 20 - Ítem 17.

Solicitamos ampliar el requisito para permitir integración con servicios de directorio equivalentes, teniendo en cuenta que actualmente las organizaciones utilizan diferentes plataformas de identidad.

Por lo que limitar el requisito únicamente a Active Directory puede restringir la participación de soluciones que soportan otros servicios de identidad ampliamente utilizados.

RESPUESTA COMITE:

No se acoge la observación,

La entidad se permite informar que mantiene el requisito establecido en el Ítem 17, relacionado con la integración con Active Directory, teniendo en cuenta que dicha capacidad es necesaria para garantizar la integración de la solución EDR-XDR con los servicios de identidad, administración de usuarios, grupos y políticas requeridos por la Entidad.

El requisito no limita que la solución ofertada cuente adicionalmente con otros mecanismos de integración con servicios de directorio, autenticación o identidad; sin embargo, para efectos del cumplimiento técnico mínimo, la solución deberá soportar integración con Active Directory.

En consecuencia, se mantiene el requisito en los términos establecidos en el Estudio Previo y no se modifica la especificación técnica mínima.

6. OBSERVACION:

OBSERVACIÓN No. 6
CONFIGURACIÓN DE PROXY
Referencia: Página 21 - Ítem 44.

Solicitamos permitir mecanismos equivalentes para la administración de conectividad de los agentes, ya que no todos los fabricantes utilizan configuración Proxy de la misma manera.

Algunos emplean conexiones directas cifradas o mecanismos automáticos de comunicación. Lo importante es garantizar la conectividad segura.

RESPUESTA COMITE:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 44 corresponde a una capacidad funcional requerida para garantizar la correcta comunicación de los agentes y de la consola de administración en entornos donde la Entidad utilice servicios proxy para el acceso a redes

externas, actualizaciones, servicios de reputación, inteligencia de amenazas o servicios en nube.

Por lo tanto, no se exige una arquitectura específica de fabricante, sino que la solución ofertada permita configurar o soportar mecanismos de proxy para los agentes y para la administración de la plataforma, de manera que se garantice la conectividad, comunicación segura, actualización y operación continua de la solución EDR-XDR.

En consecuencia, el requisito se mantiene en los términos establecidos.

7. OBSERVACION:

OBSERVACIÓN No. 7
REQUISITOS DE SEGURIDAD DE CORREO ELECTRÓNICO AJENOS AL LICENCIAMIENTO BASE DEL XDR
Referencia: Ítems relacionados con Email Profile, acciones sobre correo electrónico, cuarentena, eliminación de mensajes y bloqueo de remitentes.

Respetuosamente solicitamos a la Entidad revisar la redacción de los requisitos relacionados con la seguridad del correo electrónico, permitiendo que estas funcionalidades puedan cumplirse mediante integración con la plataforma de correo que posea la solución ofertada.

Esto teniendo en cuenta que las funcionalidades solicitadas corresponden a una solución especializada para proteger el correo electrónico y no hacen parte, de manera general, del licenciamiento básico de una plataforma XDR.

A manera de ejemplo, sería equivalente a solicitar un vehículo y exigir que, dentro del mismo precio, también se incluya un sistema especializado de monitoreo satelital. Aunque ambos trabajan conjuntamente para mejorar la seguridad, corresponden a productos diferentes.
Mantener este requisito como obligatorio dentro del licenciamiento base obliga a los oferentes a adquirir componentes adicionales, incrementando el costo de la solución y reduciendo la participación de fabricantes que cumplen el objetivo mediante integración con plataformas de correo ya existentes.

Por lo anterior, solicitamos permitir que estas funcionalidades puedan acreditarse mediante integración con soluciones de correo compatibles con la arquitectura ofertada, preservando plenamente la necesidad funcional de la Entidad y promoviendo la pluralidad de oferentes.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que los requisitos relacionados con seguridad de correo electrónico hacen parte del alcance funcional esperado para la solución EDR-XDR, en el marco de las capacidades de correlación, investigación, respuesta y visibilidad multidominio requeridas por la Entidad.

Por lo tanto, no se está exigiendo una solución de correo electrónico independiente ni una arquitectura específica de fabricante. No obstante, la solución ofertada deberá contar con capacidades nativas, integradas o soportadas oficialmente que permitan analizar, correlacionar y responder frente a eventos asociados al correo electrónico, conforme a las especificaciones técnicas mínimas del proceso.

En consecuencia, el requisito se mantiene, aclarando que podrá cumplirse mediante funcionalidades propias de la plataforma XDR o integraciones oficiales incluidas dentro de la solución ofertada, siempre que se garantice el cumplimiento técnico requerido por la Entidad.

8. OBSERVACION:

OBSERVACIÓN No. 8
CLASIFICACIÓN DE SEVERIDAD
Referencia: Página 21 - Ítem 43.

Solicitamos permitir esquemas equivalentes para la clasificación de eventos, ya que cada fabricante utiliza metodologías diferentes para priorizar alertas. Algunos manejan niveles Alto, Medio y Bajo; otros emplean puntuaciones de riesgo o criticidad.

La Entidad debe exigir la capacidad de priorizar eventos, no una clasificación específica.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 43 tiene como finalidad garantizar que la solución permita clasificar, visualizar y notificar los eventos de seguridad de acuerdo con su criticidad o nivel de severidad.

Por tal motivo, no se pretende limitar el cumplimiento a una nomenclatura exclusiva de fabricante; sin embargo, la solución ofertada deberá permitir identificar y diferenciar eventos por niveles de criticidad tales como High, Medium, Low o su equivalente funcional, de manera que se facilite la priorización, atención y gestión de incidentes de seguridad.

En consecuencia, el requisito se mantiene en los términos establecidos, aclarando que la clasificación podrá ser presentada mediante niveles de severidad, riesgo o criticidad, siempre que permita cumplir el objetivo técnico requerido por la Entidad.

9. OBSERVACION:

OBSERVACIÓN No. 9
PROGRAMACIÓN DE SINCRONIZACIÓN
Referencia: Página 21 - Ítem 38.

Solicitamos permitir mecanismos automáticos equivalentes para la sincronización de políticas.

Actualmente muchas plataformas sincronizan automáticamente la información sin necesidad de programación manual. Exigir un método específico puede excluir arquitecturas más modernas.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 38 corresponde a una funcionalidad básica de administración de la solución, orientada a permitir la programación, sincronización y aplicación controlada de políticas sobre los equipos protegidos.

Dicha capacidad resulta necesaria para garantizar una gestión ordenada de la plataforma EDR-XDR, facilitar la administración de los agentes y asegurar que las políticas de seguridad sean aplicadas de manera oportuna conforme a las necesidades operativas de la Entidad.

En consecuencia, el requisito se mantiene en los términos establecidos en el Estudio Previo, al corresponder a una funcionalidad mínima de administración y operación de la solución ofertada.

10. OBSERVACION:

OBSERVACIÓN No. 10
REQUISITOS DE ANALÍTICA DE RED Y NDR BASADOS EN COMPONENTES ESPECIALIZADOS
Referencia: Ítems 173 al 184, página 26 del documento estudio previo definitivo.

Solicitamos revisar los requisitos relacionados con analítica avanzada de red, detección de movimiento lateral y monitoreo del tráfico de la red.
Las funcionalidades descritas corresponden a herramientas especializadas cuyo propósito exclusivo es analizar el comportamiento del tráfico de la red corporativa.

Estas herramientas normalmente constituyen productos independientes y no hacen parte del licenciamiento básico de una solución XDR.

Como ejemplo, sería similar a adquirir un sistema de videovigilancia y exigir que dentro del mismo contrato se incluya también un sistema completo de control de acceso biométrico. Ambos fortalecen la seguridad, pero corresponden a soluciones distintas.
La necesidad de la Entidad es contar con información suficiente para investigar incidentes de seguridad. Ese objetivo puede alcanzarse mediante integración con herramientas equivalentes, sin exigir obligatoriamente un componente especializado adicional.

Por lo anterior, solicitamos permitir que estas capacidades puedan ser suministradas mediante mecanismos equivalentes de integración, preservando el objetivo funcional del proceso y garantizando una mayor pluralidad de oferentes.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

El comité técnico estructurador se permite informar que mantiene los requisitos relacionados con analítica de red, toda vez que dichas capacidades son necesarias para fortalecer la visibilidad, correlación e investigación de eventos de seguridad desde la perspectiva de red, complementando la información obtenida desde los endpoints.

Las funcionalidades solicitadas permiten identificar comunicaciones sospechosas, movimientos laterales, conexiones de comando y control, descargas maliciosas, direccionalidad del tráfico, protocolos utilizados y relación entre hosts internos y externos, elementos relevantes para la detección y respuesta frente a incidentes de seguridad.

En consecuencia, se mantiene el requisito en los términos establecidos en el Estudio Previo, al corresponder a una capacidad técnica requerida para la operación integral de la solución EDR-XDR.

11. OBSERVACION:

OBSERVACIÓN No. 11
MIGRACIÓN ENTRE VERSIONES
Referencia: Página 20 - Ítem 18.
Solicitamos ajustar el requisito para permitir procedimientos equivalentes de actualización.

Teniendo en cuenta que cada fabricante implementa sus procesos de actualización de manera diferente y lo importante es garantizar la continuidad del servicio y la conservación de la información.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 18 corresponde a una funcionalidad mínima requerida para garantizar que la solución permita realizar procesos de migración o actualización a versiones superiores, conservando las configuraciones y la información asociada a la administración de la plataforma.

La Entidad no exige un procedimiento específico de fabricante; sin embargo, la solución ofertada deberá garantizar la continuidad del servicio, la conservación de configuraciones y la integridad de la información durante los procesos de actualización o migración de versión.

En consecuencia, el requisito se mantiene en los términos establecidos en el Estudio Previo.

12. OBSERVACION:

OBSERVACIÓN No. 12
PROTECCIÓN FRENTE A DESINSTALACIÓN
Referencia: Página 22 - ítem 46.

Solicitamos permitir mecanismos equivalentes de autoprotección, ya que los fabricantes implementan esta funcionalidad mediante diferentes tecnologías y lo relevante es impedir la desinstalación no autorizada y proteger la integridad del agente.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 46 corresponde a una funcionalidad mínima de autoprotección del agente de seguridad instalado en los endpoints.

Dicha capacidad es necesaria para evitar la desinstalación no autorizada, cancelación de procesos, manipulación o des habilitación de los componentes de protección por parte de usuarios o aplicaciones de terceros, garantizando la continuidad operativa de la solución EDR-XDR y la protección permanente de los equipos.

En consecuencia, el requisito se mantiene en los términos establecidos en el Estudio Previo, aclarando que corresponde a una capacidad funcional de seguridad del agente y no a una arquitectura específica de fabricante.

13. OBSERVACION:

OBSERVACIÓN No. 13
UTILIZACIÓN DE NOMENCLATURAS Y CONCEPTOS PROPIETARIOS DE PLATAFORMAS XDR ESPECÍFICAS
Referencia: ítems 101 al 208, páginas 24 a 27 del documento estudio previo definitivo.

Solicitamos revisar la utilización de algunos términos y conceptos que corresponden a la forma en que determinados fabricantes implementan sus funcionalidades.

En los procesos de contratación pública es recomendable que los requisitos describan qué necesita la Entidad y no cómo un fabricante específico implementa esa necesidad.

Por ejemplo, si una Entidad requiere imprimir documentos, lo adecuado es solicitar una "impresora láser o equivalente" y no exigir el nombre comercial de una función utilizada únicamente por un fabricante determinado.

De igual forma, en este proceso resulta más conveniente describir capacidades como investigación de incidentes, análisis de causa raíz, correlación de eventos y respuesta ante amenazas, evitando referencias a metodologías o nomenclaturas propias de plataformas específicas.
Con este ajuste se mantiene exactamente la misma necesidad funcional de la Entidad, pero se amplía la participación de diferentes fabricantes que ofrecen capacidades equivalentes, fortaleciendo los principios de pluralidad de oferentes y selección objetiva.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar a la observación presentada y precisa que los requerimientos técnicos del proceso fueron definidos con fundamento en los principios de transparencia, selección objetiva, economía, responsabilidad y libre concurrencia previstos en la Ley 80 de 1993. Dichos requisitos no tienen como finalidad restringir la participación de oferentes ni direccionar el proceso hacia un fabricante específico, sino garantizar que la solución contratada responda de manera adecuada a la necesidad pública identificada.

En relación con los términos empleados en los ítems 101 al 201, se aclara que estos hacen referencia a capacidades funcionales esperadas dentro de una solución EDR-XDR, orientadas a la detección avanzada, correlación de eventos, análisis de causa raíz, investigación de amenazas, búsqueda de indicadores de compromiso, gestión de respuestas, conectores, visualización de alertas y trazabilidad de acciones.

La Entidad no exige una denominación comercial particular ni una marca específica. En consecuencia, la evaluación se realizará sobre el cumplimiento técnico de las capacidades requeridas y no sobre el nombre que cada fabricante utilice para sus módulos, consolas o funcionalidades.

Por lo anterior, se mantiene el alcance funcional de los requisitos establecidos en el Estudio Previo.

14. OBSERVACION:

OBSERVACIÓN No. 14
GESTIÓN DE ROLES
Referencia: Página 21 - Ítem 36.

Solicitamos permitir modelos equivalentes de administración de usuarios y privilegios, ya que cada fabricante implementa la administración de usuarios de forma diferente, y lo importante es garantizar el control de acceso y la segregación de funciones, sin limitar la implementación a un modelo específico.

RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar al observante que el requisito establecido en el Ítem 36 corresponde a una funcionalidad básica de administración de la solución, orientada a permitir la creación, modificación y eliminación de roles y usuarios para la gestión segura de la plataforma.

Dicha capacidad es necesaria para garantizar el control de acceso, la segregación de funciones, la asignación de privilegios y la trazabilidad de las actividades realizadas por los administradores de la solución EDR-XDR.

En consecuencia, el requisito se mantiene en los términos establecidos en el Estudio Previo, al corresponder a una funcionalidad mínima de administración y seguridad de la solución ofertada.

15. OBSERVACION:

OBSERVACIÓN No. 15
REQUISITOS DE CORRELACIÓN MULTIDOMINIO OBLIGATORIA
Referencia: Páginas 24 a 28 del documento estudio previo definitivo

Solicitamos revisar el requisito que exige que el licenciamiento base de la solución incluya de manera simultánea capacidades de correlación sobre correo electrónico, estaciones de trabajo (endpoints), red, identidades, telemetría y demás dominios de seguridad.

La finalidad de una solución XDR es centralizar y correlacionar información de diferentes fuentes para facilitar la investigación y respuesta ante incidentes de seguridad. Sin embargo, no todos los fabricantes implementan esta funcionalidad de la misma manera.

Algunos fabricantes incluyen todas estas capacidades dentro de una única licencia empresarial, mientras que otros las suministran mediante componentes o integraciones que trabajan de forma conjunta, obteniendo el mismo resultado funcional.

A manera de ejemplo, sería similar a solicitar un computador con herramientas de oficina. Algunos fabricantes las entregan preinstaladas en un solo paquete, mientras que otros permiten integrarlas posteriormente sin afectar su funcionamiento. En ambos casos el usuario obtiene el mismo resultado, aunque la forma de implementarlo sea diferente.

Mantener la exigencia de que todas estas funcionalidades se encuentren obligatoriamente incluidas dentro del licenciamiento base puede limitar la participación de fabricantes que cumplen plenamente la necesidad de la Entidad mediante arquitecturas integradas o interoperables, reduciendo la pluralidad de oferentes sin generar un beneficio adicional para la operación.

Es importante resaltar que el objetivo de la Entidad no es la forma en que cada fabricante construye su plataforma, sino contar con la capacidad de correlacionar información de diferentes fuentes para detectar, investigar y responder a incidentes de seguridad.

Por lo anterior, respetuosamente solicitamos permitir que la correlación multidominio pueda acreditarse mediante componentes nativos, integrados o interoperables de la arquitectura ofertada, siempre que el resultado funcional requerido por la Entidad



RESPUESTA COMITE TECNICO:

No se acoge la observación,

La entidad se permite aclarar que la observación presentada y precisa que los requerimientos técnicos del proceso fueron definidos con fundamento en los principios de transparencia, selección objetiva, economía, responsabilidad y libre concurrencia previstos en la Ley 80 de 1993. Dichos requisitos no tienen como finalidad restringir la participación de oferentes ni direccionar el proceso hacia un proveedor específico, sino garantizar que la solución contratada responda de manera adecuada a la necesidad pública identificada.

Frente al requisito de correlación multidominio, se aclara que este corresponde a una capacidad funcional esperada dentro de la solución EDR-XDR ofertada, orientada a centralizar, correlacionar y analizar eventos provenientes de diferentes fuentes de seguridad, tales como endpoints, red, correo electrónico, identidades, servidores, telemetría y demás componentes que permitan fortalecer la detección, investigación y respuesta ante incidentes.

La Entidad no exige una arquitectura específica ni una denominación comercial particular. No obstante, la solución ofertada deberá garantizar la correlación multidominio requerida, ya sea mediante capacidades nativas, integradas o componentes oficiales de la solución presentada, de conformidad con lo establecido en las especificaciones técnicas, sin que esto represente un costo adicional para la entidad.

En consecuencia, se mantienen los ítems observados en los términos establecidos en el Estudio Previo, aclarando que la evaluación se realizará sobre el cumplimiento técnico de las capacidades requeridas y no sobre la forma particular en que cada fabricante implemente dichas funcionalidades.

INMOTIKA SAS
25/06/2026 6:24:21 PM(UTC-05:00

1. OBSERVACION:

"Observación al numeral 5.1 – Certificaciones del fabricante

Respetuosamente solicitamos a la Entidad modificar el numeral 5.1 del pliego de condiciones, en el sentido de que las certificaciones expedidas por el fabricante que acreditan la calidad de Partner, distribuidor, comercializador autorizado o Security Partner, dirigidas a la Entidad y con una vigencia determinada, sean exigibles únicamente al proponente adjudicatario como requisito previo a la suscripción del acta de inicio o, en su defecto, antes del perfeccionamiento de la ejecución contractual, y no como documento obligatorio para la presentación de la oferta. La anterior solicitud obedece a que dichas certificaciones no acreditan la capacidad jurídica, financiera, organizacional o técnica mínima del proponente para participar en el proceso de selección, sino que constituyen un requisito relacionado con la posibilidad de ejecutar el contrato mediante el suministro de garantías y soporte oficial del fabricante.

Debe tenerse en cuenta que la finalidad de la certificación es garantizar que el contratista que finalmente ejecutará el contrato cuente con el respaldo y autorización del fabricante para suministrar las renovaciones de garantía y soporte requeridas por la Entidad. Dicha finalidad se satisface plenamente exigiendo el documento al adjudicatario antes del inicio de la ejecución contractual, sin que exista riesgo para la Entidad ni afectación del cumplimiento del objeto contractual.

En consecuencia, solicitamos modificar el requisito para que las certificaciones exigidas sean presentadas exclusivamente por el proponente adjudicatario dentro del término que establezca la Entidad previo al inicio de la ejecución del contrato, garantizando de esta manera el cumplimiento del objeto contractual sin limitar injustificadamente la participación de posibles

oferentes".

RESPUESTA COMITE:

Se acoge la observación,

La entidad se permite informar que el requisito de presentar la certificación del fabricante o canal autorizado, teniendo en cuenta que dicho documento permite verificar desde la etapa de evaluación que el proponente cuenta con respaldo oficial para comercializar, renovar, implementar y/o soportar la solución ofertada.

Dado que el objeto del proceso corresponde a la renovación de licenciamiento y soporte técnico de una plataforma de seguridad, resulta necesario garantizar previamente la trazabilidad del licenciamiento, la validez de la renovación, el acceso a soporte oficial y la capacidad del oferente para gestionar adecuadamente los servicios requeridos.

Por lo tanto, dicha certificación será requerida al oferente adjudicatario al inicio de la ejecución del proceso.

DRONIFY
30/06/2026 4:38:30 PM(UTC-05:00) Bogotá, Lima, Quito)

1. PRIMERA OBSERVACION:

1. Observación al Perfil – Ingeniero de Implementación

Respetuosamente solicitamos a la Entidad modificar el requisito de experiencia del perfil **Ingeniero de Implementación**, permitiendo acreditar **mínimo un (1) año de experiencia específica**, en lugar de los dos (2) años actualmente exigidos.

Lo anterior, por cuanto la finalidad perseguida por la Entidad, según la justificación incorporada en el mismo pliego, consiste en garantizar que el profesional cuente con conocimientos actualizados sobre las últimas versiones, funcionalidades y procedimientos de implementación de la solución ofertada. Sin embargo, dicho objetivo ya se encuentra plenamente asegurado mediante la exigencia de aportar una **certificación oficial vigente del fabricante**, expedida con una antigüedad no mayor a dos (2) años respecto de la presentación de la oferta.

Las certificaciones técnicas emitidas por los fabricantes de soluciones XDR acreditan que el profesional aprobó los procesos oficiales de capacitación y evaluación sobre las versiones vigentes del producto. En consecuencia, la actualización técnica depende de la vigencia de dicha certificación y no del número de años de experiencia acreditados.

Adicionalmente, las implementaciones de soluciones XDR se desarrollan bajo metodologías estandarizadas y procedimientos definidos por el fabricante, razón por la cual un profesional certificado que haya participado al menos en un proyecto de implementación cuenta con las competencias necesarias para ejecutar adecuadamente las actividades requeridas en el contrato.

En ese sentido, exigir dos (2) años de experiencia específica resulta una condición más restrictiva que necesaria, toda vez que no incrementa objetivamente la capacidad técnica del profesional cuando éste ya demuestra:

- Formación profesional en ingeniería.

- Certificación oficial vigente del fabricante de la solución ofertada.
- Participación certificada en al menos un (1) proyecto de seguridad.
- Conocimientos actualizados sobre la tecnología, respaldados por el fabricante.

Por lo anterior, solicitamos modificar el requisito así:

"Experiencia específica mínima de un (1) año, contada a partir de la expedición de la tarjeta profesional, y participación certificada en al menos un (1) proyecto de implementación de soluciones de seguridad."

Esta modificación mantiene la idoneidad técnica del personal requerido, promueve una mayor pluralidad de oferentes y resulta acorde con los principios de proporcionalidad, selección objetiva y libre concurrencia previstos en la Ley 80 de 1993 y la Ley 1150 de 2007, sin afectar la adecuada ejecución del objeto contractual.

RESPUESTA ENTIDAD:

Se acoge la observación,

La entidad se permite aclara que, la certificación vigente del fabricante acredita que el profesional cuenta con conocimientos técnicos sobre la implementación y configuración de la solución XDR ofertada. No obstante, dicha certificación no sustituye la experiencia práctica adquirida en proyectos reales.

Por lo tanto, la experiencia mínima de un (1) año permite garantizar que el Ingeniero de Implementación cuente con capacidades para ejecutar actividades de configuración, integración, puesta en operación, ajuste de políticas, resolución de contingencias y estabilización de la solución.

Asimismo, la participación de este debe ser como mínimo un proyecto o más que permita determinar por sí mismo su alcance, duración, complejidad ni el nivel de responsabilidad asumido por el profesional, por lo tanto, el perfil del ingeniero de implementación quedara así:

ITEM	CARGO	CANT	PERFIL ACADÉMICO	EXPERIENCIA GENERAL	EXPERIENCIA ESPECIFICA
2	**INGENIERO DE IMPLEMENTACIÓN**	1	Un ingeniero de sistemas, telecomunicaciones, electrónico o afines Certificado por el fabricante de la solución ofertada, con curso en implementación y configuración de la solución de XDR de la marca ofertada.	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional, así: Minino de 01 año con el fin de garantizar que está vigente y que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante (EDR - XDR)	Experiencia certificada, como mínimo debe haber participado en 1 proyecto de seguridad. Deberá adjuntar certificado del fabricante vigente, con fecha de expedición menor a 2 años a partir de la presentación de la oferta, con el fin de garantizar que está vigente y que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante.

2. SEGUNDA OBSERVACIÓN:

2. Observación al requisito de certificación del Ingeniero de Seguridad

Respetuosamente solicitamos a la Entidad modificar el requisito de certificación del perfil **Ingeniero de Seguridad**, permitiendo acreditar indistintamente las certificaciones **FCP-NS (Fortinet Certified Professional – Network Security) y/o FCSS (Fortinet Certified Solution Specialist)**.

Lo anterior, considerando que ambas certificaciones hacen parte del programa oficial de capacitación y certificación de Fortinet y acreditan conocimientos técnicos especializados para el diseño, implementación, administración y soporte de soluciones de ciberseguridad del fabricante.

Es importante precisar que Fortinet evolucionó recientemente su esquema de certificaciones, estructurándolo en diferentes niveles de especialización, donde tanto **FCP** como **FCSS** certifican competencias profesionales sobre las tecnologías de seguridad del fabricante, orientadas a distintos alcances técnicos y escenarios de implementación. En consecuencia, exigir exclusivamente una de ellas no representa un incremento en la capacidad técnica requerida para la ejecución del contrato, pero si restringe la participación de profesionales que cuentan con certificaciones oficiales igualmente vigentes y reconocidas por el fabricante.

Permitir la acreditación mediante **FCP-NS y/o FCSS** garantiza que el profesional posea las competencias técnicas necesarias para la correcta implementación y administración de la solución ofertada, manteniendo el nivel de idoneidad requerido por la Entidad y promoviendo simultáneamente los principios de pluralidad de oferentes, libre concurrencia y selección objetiva.

Por lo anterior, respetuosamente solicitamos que el requisito quede así:

"Certificación oficial vigente del fabricante de la solución ofertada, acreditando nivel FCP-NS y/o FCSS, o su equivalente vigente dentro de la ruta oficial de certificaciones del fabricante."

Esta modificación conserva el nivel técnico exigido, se ajusta a la evolución del programa oficial de certificaciones de Fortinet y evita restricciones innecesarias que limiten la participación de oferentes sin aportar un valor técnico adicional para la adecuada ejecución del contrato

RESPUESTA ENTIDAD:

No se acoge la solicitud. El requisito fue definido durante la estructuración y publicación del proceso, momento en el cual las certificaciones FCP y FCSS correspondían a las denominaciones oficiales y vigentes establecidas por Fortinet.

La actualización del programa de certificaciones efectuada posteriormente por el fabricante no invalida las certificaciones expedidas con anterioridad ni modifica las competencias técnicas acreditadas por sus titulares. Las certificaciones activas conservan su vigencia y cuentan con la correspondiente transición dentro del nuevo esquema NSE.

En consecuencia, la Entidad considera que el requisito continúa siendo técnicamente pertinente, vigente y verificable, por lo cual se mantiene conforme fue establecido en los documentos del proceso.

CF. CLAUDIA PATRICIA PÉREZ RODRÍGUEZ
JEFE DEPARTAMENTO ADMINISTRATIVO Y ORDENADORA DEL GASTO

MY. GISEL [illegible]MERO CARO
JEFE SECCIÓN DE CONTRATOS

MY JESUS DARIO SORIA NIETO
Gerente Proyecto

TE RAMIREZ FLOR ENRIQUE
Comité Técnico Estructurador

PS. MARTHA CECILIA JULIO CORTEZ
COMITÉ JURÍDICO LIDER