

RESPUESTA A OBSERVACIONES – ANEXO 1. ESPECIFICACIONES TÉCNICAS

OBJETO: OTIC-I-004: Adquirir la suscripción de un software especializado tipo XDR Detección y respuestas extendidas para la protección autónoma en la nube y en la red para el fortalecimiento de la infraestructura tecnológica de la Secretaría Jurídica Distrital.

La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, por medio del presente documento procede a dar respuesta a las observaciones técnicas presentadas en la convocatoria de cotización de la siguiente manera:

OBSERVACIONES REDNEET S.A.S SUMINISTROS DE ACCESS POINTS

Observaciones presentadas a través de plataforma SECOP II, el día 07 de septiembre de 2026 a las 10:24 pm.

Observación No. 1

“Se solicita permitir arquitecturas SaaS multitenant o arquitecturas cloud con segregación lógica y segura de la información de cada cliente, en lugar de exigir exclusivamente arquitectura multitenant.”

Respuesta

La entidad acepta el enfoque funcional en cuanto a los mecanismos de aislamiento (segregación lógica, RBAC, separación segura de datos). Sin embargo, se mantiene que la solución sea provista bajo la modalidad SaaS directamente por el fabricante, esto con el fin de dar cumplimiento a los lineamientos de arquitectura de infraestructura, los recursos tecnológicos con los que cuenta la Entidad y poder recopilar los eventos en redes, servidores y nube en tiempo real.

En consecuencia, la Entidad acoge parcialmente la observación presentada, quedando el numeral 1 del punto 3.1 Consola Central XDR y Protección en la Nube (SaaS) de la siguiente manera:

1. La consola de administración deberá operar bajo modalidad SaaS (Software as a Service) provista directamente por el fabricante, garantizando la segregación lógica, confidencialidad, integridad y aislamiento de la información de la Entidad, mediante arquitectura multitenant o arquitectura cloud equivalente, con controles verificables de aislamiento, gestión de acceso basada en roles (RBAC) y separación segura de datos entre clientes. El oferente deberá describir y documentar la arquitectura ofrecida y sus mecanismos de aislamiento.

Observación No. 2

“ Se solicita aclarar que estas capacidades pueden ser habilitadas y configuradas durante la implementación, directamente en la plataforma o mediante integración con el proveedor de identidad de la Entidad.”

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195



Respuesta

Teniendo en cuenta que, la observación presentada no compromete el objeto ni las características técnicas a contratar, la entidad acepta parcialmente la observación presentada por el oferente y se inserta el numeral 2 1 del punto 3.1 Consola Central XDR y Protección en la Nube (SaaS) de la siguiente manera:

2. La consola deberá permitir acceso web seguro y soportar autenticación multifactor (MFA/2FA) e inicio de sesión único (SSO) mediante SAML 2.0, OpenID Connect, OAuth 2.0 o protocolos empresariales equivalentes. Estas capacidades podrán ser nativas de la plataforma o implementarse mediante integración de identidad de la Entidad, y deberán quedar configuradas y operativas durante la fase de implementación, previo a aprobación por parte del supervisor de contrato.

Observación No. 3

“Se solicita permitir correlación en tiempo real o cercana al tiempo real, dejando como obligatoria únicamente la correlación de endpoints y servidores, e incorporando red, nube e identidad solo como fuentes opcionales mediante los mecanismos propios de cada fabricante.”

Respuesta

La entidad no acepta la observación, debido a que es una necesidad la correlación multidominio (red, nube, servidores y estaciones de trabajo), adicionalmente, es un atributo propio de las soluciones XDR, que por medio de la telemetría permite visualizar, centralizar, unir y detener ataques ocultos de forma rápida y eficiente en la infraestructura tecnológica.

Observación No. 4

“Se solicita eliminar la exigencia de que todas las integraciones sean "nativas" y aceptar conectores certificados, APIs, syslog, webhooks, aplicaciones de marketplace u otros mecanismos del fabricante.”

Respuesta

La entidad acepta parcialmente la observación quedando el numeral 4 del punto 3.1 Consola Central XDR y Protección en la Nube (SaaS) de la siguiente manera:

4. La solución deberá contar con Integración con fuentes de datos de terceros (SIEM, Firewalls, OCI, Azure, AWS) mediante conectores como APIs, RESTful documentadas, syslog y marketplaces propios del fabricante.

Observación No. 5

“Se solicita modificar integralmente el requisito porque únicamente Gartner publica un “Cuadrante de Líderes”. SE Labs y AV-TEST realizan pruebas y certificaciones, pero no poseen cuadrantes de líderes.”

Respuesta

La observación es técnicamente correcta en cuanto a que SE Labs y AV-TEST otorgan certificaciones de laboratorio y no publican cuadrantes de posicionamiento de analistas; ese término corresponde únicamente a Gartner. Se corrige la redacción en ese sentido y se elimina la exigencia de presencia simultánea y continua en las tres organizaciones durante los tres (3) años: bastará con acreditar al menos una de las tres condiciones descritas a continuación. La Entidad mantiene, en todo caso, que el reconocimiento o la certificación deben referirse específicamente al mercado de EPP, EDR y/o XDR y no a categorías de mercado distintas y no equivalentes, como la Gestión Unificada de Endpoints (UEM).

En consecuencia, la Entidad acoge parcialmente la observación presentada, quedando el numeral 5 del punto 3.1 Consola Central XDR y Protección en la Nube (SaaS) de la siguiente manera:

5. La solución ofertada deberá acreditar, dentro de los últimos tres (3) años, al menos una (1) de las siguientes condiciones: (i) posicionamiento como Líder ("Leader") en el Cuadrante de Líderes del Gartner Magic Quadrant for Endpoint Protection Platforms; (ii) certificación vigente expedida por SE Labs para soluciones EPP, EDR y/o XDR; o (iii) certificación vigente expedida por AV-TEST para soluciones EPP, EDR y/o XDR. No se aceptará el reconocimiento o la certificación obtenidos en informes o pruebas referidos a categorías de mercado distintas al EPP/EDR/XDR (p. ej., Gestión Unificada de Endpoints/UEM).

Observación No. 6

“Se solicita no exigir exclusivamente que la protección anti-tamper opere “a nivel de kernel” y evaluar el resultado de seguridad obtenido, permitiendo mecanismos equivalentes.”

Respuesta

La Entidad no acoge la observación y mantiene la exigencia de que la protección contra manipulación (anti-tamper) opere a nivel de kernel. La arquitectura de los sistemas operativos modernos divide la ejecución en niveles de privilegio o "anillos" (rings): el espacio de usuario (Anillo 3), donde se ejecutan las aplicaciones convencionales, y el kernel (Anillo 0), único nivel con acceso directo y sin restricciones a la memoria del sistema y al hardware. Una protección anti-tamper que resida exclusivamente en el Anillo 3 puede ser detectada, detenida o desactivada por cualquier proceso que logre escalar privilegios hasta el Anillo 0, quedando el agente de seguridad

completamente indefenso frente a esa amenaza.

Observación No. 7

“Se solicita evitar la obligación absoluta de no requerir reinicio del sistema, dado que esta condición puede depender del sistema operativo, versión del agente o componentes involucrados.”

Respuesta

La entidad acepta parcialmente la observación presentada, quedando el numeral 3 del punto 3.2. Agente Unificado y Compatibilidad del a siguiente manera:

3. La instalación y las actualizaciones ordinarias del agente deberán realizarse de manera transparente y, generalmente, sin requerir reinicio del sistema. En caso de que el sistema operativo, una actualización de componentes, controladores o prerequisites técnicos requiera reinicio, este deberá ser informado y coordinado con la supervisión del contrato.

Observación No. 8

“Se solicita separar las capacidades de respuesta y aceptar mecanismos equivalentes de remediación y recuperación.”

Respuesta

La entidad no acepta la observación y le aclara al oferente que la función de “rollback” (Reversión) es una característica que debe tener la solución y no es la única que se pide en este requerimiento ya que también se solicita que debe tener funciones como aislar endpoints de la red, cancelar procesos maliciosos y bloquear tráfico malicioso en la red o nube de forma automática.

Observación No. 9

“Se solicita permitir que el bloqueo sea ejecutado directamente por la plataforma o mediante integración con controles de seguridad existentes.”

Respuesta

La entidad no acepta la observación, debido a que esta busca reducir el tiempo de exposición, evitar los movimientos laterales, disminución de falsos positivos entre otros. Adicionalmente, la entidad no cuenta con herramientas tipo SOAR, que permitan automatizar procesos con otras soluciones de seguridad existentes en la Entidad.

Observación No. 10

“Se solicita distinguir entre prevención local offline y acciones remotas de mitigación, las cuales requieren restablecer la comunicación con la consola.”

Respuesta

La entidad acepta parcialmente la observación presentada, quedando el numeral 3 del punto 3.3. Protección Autónoma y Respuesta Automatizada (SOAR/XDR) de la siguiente manera:

3. La solución instalada en los dispositivos deberá contar con la capacidad de prevención y mitigación de amenazas en estado desconectado (offline).

Observación No. 11

“Se solicita aclarar que las integraciones estarán sujetas a la disponibilidad de accesos, licencias, APIs, permisos y colaboración de la Entidad.”

Respuesta

La entidad aclara al oferente, que la solución se deberá integrar contra el directorio activo de la entidad por los conectores expuestos en el numeral 4 del punto 3.1 Consola Central XDR y Protección en la Nube (SaaS). Adicionalmente, se establecerán mesas de trabajo con el futuro contratista para que de forma armónica que realice la implementación de la solución.

Observación No. 12

“Validación de soluciones disponibles en el IAD/SDA de Software por Catálogo II”

Respuesta

La entidad no acepta la observación, en el entendido que las soluciones incorporadas dentro del Instrumento de Agregación de Demanda/Sistema Dinámico de Adquisición de Software por Catálogo II, no se incluyen soluciones específicas de XDR, razón por la cual la entidad se encuentra adelantando un estudio de mercado de forma alterna a este mecanismo de contratación.

Por otra parte, la solución *“ManageEngine”* no incluye dentro de sus servicios y como propósito soluciones XDR, esta cuenta con productos como Endpoint Central (UEM + EDR) y Log360 (SIEM/SOAR) los cuales no cumplen con el alcance técnico que busca la entidad.

OBSERVACIONES DATAMOTION SAS

Observaciones presentadas a través de plataforma SECOP II, el día 08 de septiembre de 2026

Observación No. 1

“Con el fin de garantizar el 100% de la cobertura de la solución y dimensionar adecuadamente los agentes tecnológicos requeridos, solicitamos amablemente a la entidad aclarar: ¿Cuáles son las versiones exactas de los sistemas operativos considerados como "legacy", ¿cuál es la cantidad de equipos que los ejecutan y si estos se encuentran incluidos dentro de las 251 estaciones de trabajo o los 30 servidores objeto de este contrato?”

Respuesta

La entidad aclara al oferente que la definición legacy hace referencia a sistemas operativos antiguos u obsoletos que no actualmente ya no cuentan con soporte del fabricante. Las versiones de sistemas operativos que tiene la entidad y estarían fuera del soporte por parte del fabricante en la ejecución del contrato son Windows server 2016, Windows 10 y Oracle Linux 7. Con respecto a la cantidad de equipos tanto físicos como virtuales con sistemas operativos son diez (10) Windows 10, seis (6) Windows server 2016 y catorce (14) Oracle Linux 7 que se encuentran dentro de la totalidad de las suscripciones que la entidad necesita adquirir.

Observación No. 2

“Consultamos a la entidad: ¿El alcance de la presente contratación exige que el oferente provea el licenciamiento y almacenamiento necesario para la ingesta activa de estas fuentes de terceros, o la solución solicitada únicamente debe contar con la capacidad técnica/arquitectura (APIs/conectores) para realizar dicha integración en caso de que la entidad lo requiera en el futuro?”

Respuesta

La entidad aclara al oferente que una de las necesidades de los servicios a contratar es que la solución cuente con conectores para la integración con fuentes de datos de soluciones que tenga la entidad. Adicionalmente se aclara que fue ajustado el numeral 4 del punto 3.1 Consola Central XDR y Protección en la Nube (SaaS) de la siguiente manera:

4. La solución deberá contar con Integración con fuentes de datos de terceros (SIEM, Firewalls, OCI, Azure, AWS) mediante conectores como APIs, RESTful documentadas, syslog y marketplaces propios del fabricante.

Observación No. 3

“solicitamos a la entidad respetuosamente aceptar que la fase de pruebas y puesta en marcha inicial se realice mediante un esquema de suscripción temporal tipo Trial/PoC de hasta treinta (30) días provisto por el fabricante, y que las suscripciones definitivas de producción por doce (12) meses sean activadas formalmente al día siguiente de la aprobación a satisfacción de dicha fase de pruebas.”

Respuesta

La entidad aclara al oferente, que el requerimiento busca que el tiempo de suscripción de la solución adquirida por la entidad no sea utilizado parcialmente en la fase de implementación, en el entendido que es un periodo que no se daría el uso completo y adecuado y reduciría el periodo de aprovechamiento. En ese sentido, se solicita se implemente mecanismos tipo demo para la fase de implementación una vez esta termine y sea aprobada por la supervisión del contrato se procederá con el proceso de activación de la suscripción adquirida.

Observación No. 4

“Se solicita respetuosamente a la entidad confirmar que el tiempo de “solución de 12 horas” se dará por cumplido mediante la aplicación de medidas de mitigación o contención temporal (como el aislamiento del endpoint o rollback del cambio) que eliminen el riesgo crítico en la entidad, mientras el fabricante genera el parche definitivo.

- Se solicita respetuosamente a la entidad aclarar que la atención en el sitio (presencial) aplicará únicamente cuando el incidente crítico no pueda ser abordado de forma remota y esté estrictamente relacionado con fallas en la implementación o parametrización local del software.”

Respuesta

La Entidad no acoge la observación, debido a que la propuesta de dar por cumplido el tiempo de "solución de 12 horas" mediante la aplicación de una medida de mitigación o contención temporal (aislamiento del endpoint, rollback del cambio), mientras el fabricante desarrolla el parche definitivo, sin plazo definido desnaturaliza el concepto mismo de "solución" exigido en el Anexo Técnico y sustituye una obligación de resultado por una obligación de simple gestión del síntoma.

Aunado a lo anterior este requerimiento se fundamenta en el marco de gestión de servicios de TI ITIL v4, que diferencia de forma clara entre los conceptos Workaround (solución temporal) y resolución.

Es importante aclarar, que en caso de que el periodo de solución supere el tiempo solicitado el futuro contratista deberá justificar la extensión de la solución para que esta sea evaluada por el supervisor de contrato.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195



Por otra parte, se aclara que la atención en sitio es una de las opciones para la prestación de servicios de soporte y no se puede limitar a que esta solo sea “cuando el incidente crítico no pueda ser abordado de forma remota y esté estrictamente relacionado con fallas en la implementación o parametrización local del software. En consecuencia, la Entidad no acoge la observación presentada.