



RESPUESTA A OBSERVACIONES DE CARÁCTER TÉCNICO

Proceso de Selección Subasta Inversa SCRD-SASI-36-2026

Objeto: Adquirir una solución de Gestión de Accesos Privilegiados (PAM) para la administración, control, monitoreo y auditoría de acceso

Respuesta a observaciones Empresa TlcXAR

1. ¿La entidad acepta que la solución se componga de varios productos integrados (incluido software de código abierto), siempre que cumpla funcionalmente los requisitos? De no ser así, ¿en qué requisito se fundamenta?

La Entidad no acoge la solicitud en los términos planteados.

La solución ofertada deberá acreditar el cumplimiento integral de las condiciones técnicas, de seguridad, arquitectura, certificación, soporte e integración establecidas en el Anexo Técnico y demás documentos del proceso.

De igual manera, de conformidad con las condiciones establecidas para el presente proceso, no se aceptará la utilización de software de código abierto dentro de la solución ofertada.

En consecuencia, no se modifican las condiciones establecidas en los documentos del proceso.

2. ¿Se aceptará software de código abierto con soporte del integrador o de un tercero? ¿Cómo se acreditaría el soporte del fabricante?

La Entidad no acepta la utilización de software de código abierto para la solución objeto del presente proceso.

La solución ofertada deberá cumplir con las condiciones técnicas, de soporte, certificación y respaldo establecidas en el Anexo Técnico y demás documentos del proceso, incluyendo los requisitos previstos para la solución PAM ofertada.

En consecuencia, no se aceptará que el cumplimiento de dichos requisitos se acredite únicamente mediante soporte de un integrador o de un tercero sobre componentes de código abierto.

Por lo anterior, no se modifica lo establecido en los documentos del proceso.





3. El estudio de mercado registra tres cotizaciones. ¿Pueden publicar las marcas y los módulos cotizados para entender el alcance base del presupuesto?

La Entidad aclara que las cotizaciones utilizadas como insumo para la determinación del presupuesto oficial se encuentran publicadas dentro de los documentos del proceso en SECOP II y pueden ser consultadas directamente por los interesados.

Se precisa que dichas cotizaciones corresponden a referentes comerciales obtenidos para la elaboración del estudio de mercado y fueron solicitadas teniendo en cuenta las condiciones técnicas definidas por la Entidad para la adquisición de la solución PAM.

En todo caso, las marcas, referencias o denominaciones comerciales que puedan encontrarse contenidas en las cotizaciones no constituyen condiciones técnicas obligatorias ni determinan la solución que deberá ser ofertada. El alcance técnico exigible a los proponentes corresponde a las características, funcionalidades, cantidades y demás requisitos establecidos en el Anexo Técnico y en los demás documentos del proceso.

Por lo anterior, la Entidad considera que la información publicada en SECOP II resulta suficiente para identificar los referentes comerciales utilizados en el estudio de mercado, precisando que el alcance y las condiciones técnicas exigibles para la presentación de las ofertas corresponden a las establecidas en el Anexo Técnico y en los demás documentos del proceso.

4. ¿Los módulos SAPM, AAPM, PSM y SUPM son obligatorios todos desde el inicio, o se puede implementar de forma modular y por fases?

La Entidad aclara que los módulos SAPM, AAPM, PSM y SUPM forman parte obligatoria de la solución requerida y deberán estar incluidos dentro de la oferta.

La totalidad de las capacidades exigidas deberá quedar implementada y disponible con la puesta en marcha y activación de la solución, dentro del plazo de ejecución contractual establecido.

Por lo anterior, no se contempla su entrega o implementación mediante fases posteriores al plazo contractual.

5. ¿Qué significa "usuario" en las 10 licencias? ¿Son 10 administradores nominales, 10 sesiones concurrentes o 10 identidades privilegiadas?

Cada una de las 10 licencias estará asignada de forma individualizada al personal técnico autorizado de la entidad (usuario). Estos usuarios utilizan sus cuentas para autenticarse en el sistema PAM y, desde allí, iniciar de forma segura sus sesiones de administración, operación y control sobre los servidores, bases de datos o servicios críticos del ecosistema tecnológico definido para esta solución.





6. ¿Cuántos sistemas objetivo se deben gestionar, por tipo (Windows, Linux, Oracle, mainframe, red, nube, aplicaciones)? ¿Cuántas cuentas privilegiadas?

La solución ofrecida deberá tener la capacidad técnica nativa de soportar e integrarse con los tipos de sistemas objetivo descritos en el Anexo Técnico: servidores Windows, UNIX/Linux, Oracle, Mainframe IBM, dispositivos de red, servicios en la nube y plataformas web.

Para efectos del dimensionamiento del proceso, se estima un alcance de aproximadamente ciento diez (110) servidores. Respecto de Mainframe IBM, actualmente la Entidad no cuenta con esta plataforma en operación; sin embargo, la solución deberá contar con la capacidad técnica para soportarla, conforme a lo establecido en el Anexo Técnico.

En cuanto al licenciamiento solicitado, las diez (10) licencias corresponden a diez (10) administradores nominales autorizados para utilizar la solución PAM. La cantidad de cuentas privilegiadas a gestionar estará determinada por las cuentas asociadas a los sistemas objetivo comprendidos dentro del alcance de la solución.

7. ¿Qué versiones y motores de bases de datos tiene la entidad? ¿Existe un mainframe IBM en operación?

Los motores de bases de datos que posee la entidad y que forma parte del alcance del proyecto corresponden a plataformas Oracle (versiones 19c, 12cR1, 10gR2), Postgres (versiones 17, 15, 13, 10.4, 9.6), MariaDB (versiones 10.11.6, 10.5.11, 10.5) y MySQL; respecto al Mainframe IBM, se aclara que actualmente la entidad no cuenta con esta plataforma en operación, sin embargo, la solución PAM ofrecida debe cumplir con la capacidad técnica nativa de soportarlo a futuro conforme a lo solicitado en el numeral 2 del anexo técnico.

8. ¿Cuántas aplicaciones requieren gestión aplicación a aplicación (AAPM) y en qué lenguajes?

La solución ofrecida debe incluir de forma obligatoria y nativa el módulo AAPM con el fin de tenerlo disponible por si se requiere su uso durante la ejecución del proyecto, toda vez que la entidad posee en su ecosistema de APIs, aplicaciones y servicios integraciones basadas en lenguajes Python, PHP, Java, Node.js, entornos estáticos HTML/Nginx, así como las tecnologías WordPress, Moodle, Gutenberg, Wiki.js, Meilisearch, Pentaho Server CE, DataHub, Highcharts Server y MongoDB.

9. ¿Qué plataformas ya existen en la entidad (directorío activo, SIEM, ITSM, EDR/XDR, SOAR, virtualización, nube)? ¿Con cuáles debe integrarse la solución?

Las plataformas que ya existen en la entidad y con las cuales debe integrarse la solución PAM son:

- Servidores Windows
- Servidores UNIX/LINUX
- Servidores ORACLE

- Dispositivos de red
- Servicios en la nube
- Plataformas WEB de diferentes Fabricantes

Respecto de Mainframe IBM, actualmente la Entidad no cuenta con esta plataforma en operación, sin embargo, la solución ofertada debe soportar esta plataforma.

10. ¿Se aceptan certificaciones equivalentes a Common Criteria? ¿Se acepta que la certificación se acredite a nivel de módulo criptográfico y no del producto completo?

No es procedente la aceptación de certificaciones equivalentes a Common Criteria, así como tampoco se acepta que la certificación se acredite únicamente a nivel de módulo criptográfico.

De acuerdo con lo establecido en el anexo técnico, la solución ofertada debe contar con la certificación Common Criteria aplicada de manera integral al producto completo. Acreditar la certificación solo en un componente o módulo criptográfico fragmenta el análisis de seguridad y desestima la evaluación global de la plataforma unificada exigida por la entidad.

Por lo anterior no se acepta la solicitud planteada por el observante.

11. ¿Se acepta FIPS 140-2 o 140-3 del módulo criptográfico (por ejemplo, un HSM validado) en lugar de la validación de todo el producto?

Una vez revisada la observación, la Entidad aclara que se aceptará la validación bajo los estándares FIPS 140-2 o FIPS 140-3.

El requisito se entenderá cumplido cuando la solución ofertada opere utilizando módulos criptográficos validados bajo alguno de los estándares señalados, cuya validación pueda ser verificada mediante la documentación o fuente oficial correspondiente.

Por lo anterior, no se exigirá que la solución PAM cuente con un certificado CMVP propio, y se realizará el ajuste correspondiente en el Anexo Técnico para precisar el alcance del requisito.

12. ¿Se acepta el despliegue en máquinas virtuales o contenedores en lugar de un appliance virtual en formato OVA, KVM o VHD?

La entidad requiere que la solución PAM sea provista mediante un appliance virtual en formato OVA, KVM o VHD, el cual debe ser completamente compatible con la infraestructura disponible en la entidad. Los proponentes deben asegurar la entrega de la solución bajo esta modalidad de despliegue para garantizar la correcta integración, soporte y estabilidad de la plataforma desde el inicio del contrato.

Por lo anterior no se acepta la solicitud planteada por el observante.

13.El requisito de "no requerir motores de base de datos ni sistemas operativos" ¿es excluyente? ¿Qué riesgo busca mitigar?

La solución ofertada debe proveerse obligatoriamente como un Appliance Virtual (en formatos OVA, KVM o VHD), incluyendo de forma nativa e integrada tanto el sistema operativo como el motor de base de datos embebido y endurecido de fábrica, sin requerir el licenciamiento ni la instalación independiente de estos componentes.

El riesgo que se busca mitigar: Evitar que personal externo altere o configure manualmente el sistema operativo o la base de datos, garantizando que el producto las mantenga íntegras, adicionalmente mitigar el riesgo de ataques dirigidos al eliminar sistemas operativos expuestos o bases de datos comerciales estándar mal configuradas, utilizando en su lugar un entorno cerrado y endurecido (*hardened*) por el propio fabricante del PAM.

Por lo anterior no se acepta la solicitud planteada por el observante.

14.¿Se acepta una arquitectura de alta disponibilidad activo-pasivo con replicación y recuperación automática en lugar de activo-activo con replicación transaccional distribuida?

De acuerdo con lo establecido en el anexo técnico, la solución debe contar de forma nativa con una arquitectura de clúster activo-activo con replicación transaccional distribuida. No es procedente la adopción de un esquema activo-pasivo, ya que la entidad requiere garantizar la alta disponibilidad simultánea, el balanceo de carga en tiempo real y la tolerancia a fallos inmediatos sin tiempos de espera ni ventanas de conmutación para la operación de la plataforma PAM.

Por lo anterior no se acepta la solicitud planteada por el observante.

15.El requisito de herramientas tipo PRTG, MRTG o Cacti con consumo de ancho de banda ¿aplica a la solución PAM o a un servicio de conectividad? Solicitamos aclarar su alcance.

Una vez revisada la observación, la Entidad aclara que se modificará el numeral 10 del Anexo Técnico, con el fin de alinear el requerimiento de monitoreo con las capacidades nativas de la solución PAM. En consecuencia, el texto quedará redactado de la siguiente manera:

“10. Plataforma gráfica: Acceso web 7x24 a la consola de la solución PAM, que permita consultar en tiempo real e histórico la disponibilidad de sus componentes, el estado de las sesiones privilegiadas y demás indicadores relevantes del servicio.”

16. ¿Los requisitos de analítica de comportamiento con aprendizaje continuo, suspensión automática de cuentas y correlación con EDR/XDR son obligatorios o deseables? ¿Cómo se verificarán en la evaluación?

La Entidad aclara que las capacidades de analítica de comportamiento, aprendizaje automático y demás funcionalidades previstas en los numerales correspondientes del Anexo Técnico forman parte de los requisitos técnicos obligatorios de la solución PAM.

Su cumplimiento deberá acreditarse mediante la documentación técnica correspondiente a la solución ofertada, de conformidad con las condiciones de verificación establecidas en los documentos del proceso.

De acuerdo a lo anterior, dichas funcionalidades no tienen carácter opcional o deseable, sino que hacen parte del alcance técnico requerido.

17. ¿Cómo se verificará el cumplimiento de los requisitos técnicos? ¿Con demostración, prueba de concepto, fichas técnicas o declaración del oferente?

La verificación del cumplimiento de los requisitos técnicos se realizará de manera obligatoria mediante la revisión de las fichas técnicas, certificados y manuales oficiales emitidos directamente por el fabricante de la solución. Los proponentes deberán adjuntar dicha documentación oficial dentro de su oferta técnica para sustentar y acreditar de forma objetiva cada una de las características solicitadas en el anexo técnico (incluyendo el modelo de licenciamiento unificado, la arquitectura y las certificaciones Common Criteria).

18. Las certificaciones exigidas son "del fabricante de la solución". Si la solución es abierta o compuesta, ¿se aceptan certificaciones en las tecnologías ofertadas, o equivalentes en seguridad e infraestructura?

Conforme a lo establecido en el anexo técnico, las certificaciones exigidas deben ser emitidas de forma directa y oficial por el fabricante único de la solución PAM unificada.

Por lo anterior no se acepta la solicitud planteada por el observante.

19. La experiencia habilitante se describe como gestión de identidades, mientras los perfiles piden experiencia en PAM. ¿Se aceptan contratos de gestión de identidades, acceso o secretos como experiencia válida?

Sí se aceptan conforme a lo establecido textualmente en los estudios previos, los contratos aportados para



acreditar la experiencia habilitante del proponente serán válidos siempre que contemplen actividades relacionadas, como mínimo, con la administración, adquisición, renovación, personalización, actualización y/o soporte de soluciones tecnológicas de gestión de identidades y/o usuarios privilegiados.

20. ¿El Gerente de Proyectos y el Especialista en Seguridad deben ser personas distintas y con dedicación exclusiva? ¿Qué porcentaje de dedicación se espera?

El Gerente de Proyectos y el Especialista en Seguridad deben corresponder a personas distintas, cuyo porcentaje de dedicación exclusiva 100% aplicará de forma estricta durante la implementación y entrega satisfactoria de la solución PAM..

**21. ¿El servicio incluye soporte, actualizaciones y garantía durante los 12 meses?
¿Cuáles son los niveles de servicio (SLA) esperados y qué cubre la bolsa de 50 horas?**

Los niveles de servicio (SLA) esperados se determinan en los tiempos de respuesta y solución necesarios para asegurar el cumplimiento, la estabilidad y el éxito operativo en la instalación e implementación de la plataforma en la entidad durante el plazo de ejecución establecido. Por su parte, la bolsa de 50 horas cubre de forma complementaria cualquier actividad, requerimiento técnico o evento relacionado de forma directa con el soporte de la solución PAM.

22.22. ¿Quién proveerá la infraestructura (servidores, almacenamiento, HSM): la entidad o el contratista? ¿Se debe incluir en el valor ofertado?

La entidad proveerá la infraestructura correspondiente a las máquinas virtuales y el almacenamiento para la ejecución del proyecto. Por su parte, el Módulo de Seguridad de (HSM) deberá ser provisto en su totalidad por el contratista/proveedor.

Respecto al valor ofertado, el costo del módulo HSM debe estar incluido dentro del valor total de la oferta presentada por el proponente.

23. ¿Qué ocurre con la solución al terminar los 12 meses? ¿Se espera continuidad, transferencia de conocimiento o entrega de documentación y código de configuración?

La Entidad aclara que la solución será adquirida bajo modalidad de suscripción por un periodo de doce (12) meses contados a partir de su activación.

Una vez finalice dicho periodo, cualquier eventual continuidad o renovación de la solución estará sujeta a las necesidades de la SCRD, la disponibilidad presupuestal y al proceso contractual que corresponda.





Respecto de la entrega de documentación, deberán atenderse las obligaciones y condiciones expresamente establecidas en el Anexo Técnico y demás documentos del proceso.

24. ¿Hay restricciones sobre el uso de software de código abierto por la política de seguridad o por licenciamiento de la entidad?

La Entidad aclara que no se aceptará software de código abierto para la solución objeto del presente proceso.

Adicionalmente, de acuerdo con el Manual de Políticas de Seguridad y Privacidad de la Información, el software utilizado deberá encontrarse debidamente licenciado y cumplir con la normativa aplicable en materia de derechos de propiedad intelectual.

Por lo anterior, cualquier solución ofertada deberá cumplir con estas condiciones y con los demás requisitos establecidos en los documentos del proceso.

25. El plazo del contrato es de treinta (30) días contados desde el acta de inicio, pero el Anexo Técnico habla de licenciamiento en suscripción por 12 meses y de una bolsa de 50 horas de soporte. ¿Cuál es el plazo total de ejecución y desde qué fecha se cuentan los 12 meses de suscripción, soporte y bolsa de horas?

La Entidad aclara que el plazo de ejecución del contrato corresponde a treinta (30) días calendario contados a partir de la suscripción del acta de inicio o documento que haga sus veces, período dentro del cual el contratista deberá realizar la entrega, implementación, parametrización, puesta en marcha y activación de la solución PAM.

Una vez realizada la activación de la solución, la SCRD adquiere el derecho de uso del licenciamiento en modalidad de suscripción por un periodo de doce (12) meses contados a partir de dicha activación, así como el derecho a utilizar la bolsa de cincuenta (50) horas de soporte técnico prevista en el Anexo Técnico durante ese mismo periodo y se encuentran incluidos dentro del valor contratado, de acuerdo con las necesidades de la Entidad.

26. ¿Cuál es el plazo máximo para entregar la solución activada e implementada? Dado que el pago es único contra la activación, instalación y configuración de las licencias, ¿los valores de implementación, gerente de proyectos, especialista y bolsa de horas se pagan dentro de ese único pago?

El plazo máximo para entregar la solución activada e implementada es de treinta (30) días calendario, conforme a lo establecido en los estudios previos. Adicionalmente, se aclara que el pago es único y se ejecutará contra la activación, instalación y configuración a satisfacción de las licencias; por lo tanto, los valores asociados a la implementación, gerente de proyectos, especialista y la bolsa de horas deben estar incluidos dentro de ese pago único, sin que haya lugar a cobros independientes o parciales.





27.El presupuesto oficial es de \$224.339.214, mientras que el CDP registra \$224.860.000. ¿Cuál es el valor de referencia para efectos del rechazo de ofertas?

La Entidad aclara que, para efectos de la presentación, evaluación y eventual rechazo de las ofertas económicas, el valor de referencia corresponde al presupuesto oficial del proceso es, DOSCIENTOS VEINTICUATRO MILLONES TRESCIENTOS TREINTA Y NUEVE MIL DOSCIENTOS CATORCE PESOS M/CTE (\$224.339.214), incluido IVA y demás impuestos, tasas, contribuciones y costos a que haya lugar.

El valor de \$224.860.000 correspondiente al CDP No. 1581 constituye la disponibilidad presupuestal que respalda el proceso de contratación y no corresponde al valor máximo de la oferta económica.

De acuerdo a lo anterior, las ofertas cuyo valor total inicial supere los \$224.339.214 serán objeto de rechazo, de conformidad con las reglas establecidas en los documentos del proceso.

29.El pliego indica que no se reconocerá ningún reajuste de precios durante la vigencia del año 2025. Como el proceso corresponde a 2026, ¿se trata de un error de redacción? Solicitamos precisar la vigencia aplicable.

La Entidad efectuará el ajuste correspondiente en el documento en el que se presenta la inconsistencia, precisando que la vigencia aplicable al presente proceso es la vigencia 2026, con el fin de mantener la coherencia de la información contenida en los documentos del proceso.

30.¿Cuáles son los amparos, porcentajes y vigencias exigidos para la garantía de cumplimiento? El pliego solo remite a los estudios previos y a SECOP II.

La Entidad aclara que los amparos, porcentajes y vigencias correspondientes a la garantía única de cumplimiento se encuentran establecidos en el numeral 12 de los Estudios Previos, documento que hace parte integral de los documentos del proceso publicados en SECOP II, así:

- Cumplimiento: por el treinta por ciento (30 %) del valor del contrato, con una vigencia igual al plazo de ejecución contractual y seis (6) meses más.
- Calidad y correcto funcionamiento de los bienes: por el veinte por ciento (20 %) del valor total del contrato, con una vigencia de doce (12) meses contados a partir de la terminación del contrato.

Adicionalmente, dentro de los requisitos de carácter jurídico se exige la garantía de seriedad de la oferta, la cual corresponde a una garantía de naturaleza precontractual y, por tanto, es independiente de los amparos que integran la garantía única de cumplimiento del contrato. Las condiciones aplicables a dicha garantía deberán atender lo establecido en los documentos del proceso y en la normativa vigente.

Por lo anterior, el proponente deberá observar tanto las condiciones de la garantía de seriedad de la oferta como los amparos, porcentajes y vigencias de la garantía única de cumplimiento establecidos en los documentos del proceso.





31. El Anexo Técnico exige que la sumatoria de los contratos sea igual o superior al presupuesto oficial, mientras que el pliego lo expresa en SMMLV. ¿Cuál prevalece? Si es en SMMLV, ¿con el salario mínimo de qué año se convierte el presupuesto oficial?

La Entidad aclara que, para efectos de la acreditación y verificación de la experiencia, se aplicará el criterio establecido, conforme al cual la sumatoria de los valores de los contratos aportados deberá ser igual o superior al presupuesto oficial establecido para el presente proceso.

De acuerdo a lo anterior, para la verificación de este requisito se tomará como referencia el presupuesto oficial del proceso, correspondiente a DOSCIENTOS VEINTICUATRO MILLONES TRESCIENTOS TREINTA Y NUEVE MIL DOSCIENTOS CATORCE PESOS M/CTE (\$224.339.214).

La Entidad efectuará el ajuste correspondiente en los documentos del proceso en los que se haga referencia a la acreditación de este requisito en SMMLV, con el fin de unificar el criterio de evaluación y mantener la coherencia entre los documentos del proceso.

32. ¿Se aceptan contratos clasificados en solo uno de los códigos UNSPSC 43231500 o 43233200? ¿Se aceptan contratos clasificados en otros códigos cuyo objeto corresponda a gestión de identidades, accesos, secretos o usuarios privilegiados? ¿Se pueden acumular contratos con alcance parcial (por ejemplo, uno de licenciamiento y otro de soporte) y contratos con entidades privadas?

La Entidad aclara que, de conformidad con lo establecido en el numeral 8.3.1 de los Estudios Previos, los contratos aportados para acreditar la experiencia deberán encontrarse registrados en el Registro Único de Proponentes – RUP bajo alguno de los códigos UNSPSC 43231500 o 43233200. En consecuencia, no se requiere que un mismo contrato se encuentre clasificado simultáneamente en ambos códigos.

Para efectos del presente proceso, no se aceptarán contratos registrados únicamente bajo códigos UNSPSC diferentes a los expresamente establecidos en los documentos del proceso, aun cuando su objeto pueda guardar relación con gestión de identidades, accesos, secretos o usuarios privilegiados, toda vez que la clasificación UNSPSC definida por la Entidad forma parte de las condiciones establecidas para la acreditación de la experiencia habilitante.

Adicionalmente, los contratos aportados deberán acreditar las actividades relacionadas con la administración y/o adquisición y/o renovación y/o personalización y/o actualización y/o soporte de soluciones tecnológicas de gestión de identidades y/o usuarios privilegiados, conforme con las condiciones previstas en los documentos del proceso.

Las actividades requeridas podrán acreditarse mediante uno o varios de los contratos presentados, por lo que es procedente acumular contratos que acrediten parcialmente los componentes de experiencia exigidos, siempre que en conjunto cumplan las condiciones de número, valor, antigüedad, clasificación UNSPSC y



demás requisitos establecidos por la Entidad.

Finalmente, se aceptarán contratos celebrados tanto con entidades públicas como con particulares. No obstante, los contratos celebrados con particulares que el proponente pretenda hacer valer para acreditar la experiencia en el presente proceso deberán encontrarse inscritos y en firme en el Registro Único de Proponentes – RUP, bajo alguno de los códigos UNSPSC exigidos, y cumplir con las demás condiciones de experiencia establecidas en los documentos del proceso.

33. Frente a la certificación de distribuidor autorizado: ¿debe ser expedida por el fabricante o puede serlo por un mayorista? Si la solución integra varios componentes o tecnologías, ¿se exige la certificación de cada uno de ellos o de la solución ofertada en su conjunto?

La certificación de distribuidor autorizado deberá ser expedida directamente por el fabricante o mayorista y deberá aplicar a la plataforma ofertada en su conjunto. No se aceptarán certificaciones emitidas por intermediarios o canales de distribución secundarios que no acrediten autorización del fabricante o del mayorista autorizado.

Asimismo, dado que la Entidad exige una solución de Gestión de Accesos Privilegiados (PAM) integrada de un único fabricante bajo una sola plataforma nativa, la certificación deberá permitir verificar la autorización para comercializar la solución ofertada y el respaldo correspondiente para su implementación y soporte.

34. El Anexo Técnico lista un "Profesional certificado en soluciones PAM a implementar" y luego un "Especialista en Seguridad". ¿Son el mismo perfil? Adicionalmente, la experiencia del especialista aparece como "3 años o 2 proyectos PAM" en el pliego y como "3 años y 2 proyectos PAM" en el anexo. ¿Cuál condición aplica?

La Entidad aclara que el perfil denominado en la tabla inicial del Anexo Técnico como "Profesional certificado en soluciones de Gestión de Accesos Privilegiados (PAM) a implementar" corresponde al mismo perfil posteriormente identificado y desarrollado como "Especialista en Seguridad"; por tanto, no se trata de dos perfiles o profesionales diferentes. Con el fin de evitar interpretaciones distintas, la Entidad unificará su denominación como "Especialista en Seguridad" en los documentos del proceso.

Así mismo, frente a la experiencia requerida para dicho perfil, se precisa que la condición aplicable es la establecida en el numeral 8.3.2 de los Estudios Previos, conforme a la cual deberá acreditarse un mínimo de tres (3) años de experiencia específica, o la participación en mínimo dos (2) proyectos en soluciones de gestión de usuarios privilegiados (PAM). Se trata, por tanto, de requisitos alternativos y no acumulativos.

De acuerdo a lo anterior, la Entidad ajustará el Anexo Técnico para armonizar con los Estudios Previos y demás documentos del proceso, de manera que quede expresamente indicada la conjunción "o" entre las dos alternativas de acreditación de experiencia.





35. ¿Qué fabricantes se consideran "reconocidos" para la certificación de soporte técnico en soluciones PAM? ¿Se aceptan certificaciones equivalentes a Scrum Master Professional e ITIL v4 (por ejemplo, PSM, CSM o ITIL Foundation)?

La Entidad aclara que se considerará como fabricante reconocido aquel cuya solución cumpla con la totalidad de los requisitos técnicos, de soporte y certificación establecidos en los documentos del proceso.

Respecto de las certificaciones requeridas para el Gerente de Proyectos, para el requisito de Scrum Master se aceptarán las certificaciones Scrum Master Professional, PSM (Professional Scrum Master) o CSM (Certified Scrum Master).

Para acreditar el requisito ITIL se aceptará ITIL v4 o ITIL 4 Foundation. No se aceptarán certificaciones correspondientes a versiones anteriores del marco ITIL.

Los demás requisitos establecidos para el perfil se mantienen.

36. Frente al requisito de Common Criteria: ¿qué se entiende por "certificada dos (2) veces"? ¿Se refiere a versiones distintas del mismo producto? ¿Qué vigencia deben tener los certificados y dónde deben ser verificables?

La Entidad aclara que la expresión "certificada dos (2) veces" hace referencia a que la solución ofertada deberá acreditar al menos dos (2) certificaciones Common Criteria obtenidas mediante evaluaciones independientes, correspondientes a versiones actuales y/o anteriores de la misma solución o producto ofertado.

Las certificaciones podrán corresponder a versiones distintas de la solución, siempre que permitan verificar que pertenecen a la misma línea de producto o solución tecnológica ofrecida.

Para efectos de su acreditación, las certificaciones deberán ser verificables en fuentes oficiales, tales como el portal oficial de Common Criteria o el sitio web del esquema de certificación que las haya expedido. Cuando se trate de certificaciones correspondientes a versiones anteriores, se aceptará su consulta en los registros o históricos oficiales de productos certificados.

En consecuencia, no se exige que las dos certificaciones correspondan necesariamente a la versión actualmente ofertada ni que ambas se encuentren vigentes a la fecha de cierre, siempre que su existencia, alcance y correspondencia con la solución puedan ser verificadas oficialmente.

37. El requisito 21 exige que las llaves maestras de cifrado residan exclusivamente en un módulo HSM. ¿Se aceptan HSM virtuales o servicios de HSM en la nube (por ejemplo, Azure Key Vault Managed HSM)?

La Entidad aclara que se acepta la utilización de HSM virtuales o servicios de HSM en la nube, siempre que cumplan con las condiciones técnicas y de seguridad establecidas en el Anexo Técnico.

En todo caso, las llaves maestras de cifrado con algoritmo AES-256 o superior deberán residir





exclusivamente en el módulo HSM y deberá cumplirse con la validación FIPS exigida en los documentos del proceso, sin que esto genere costos adicionales para la entidad.

38. Los requisitos 80 a 99 corresponden a controles a nivel de kernel y de endpoint (SUPM). ¿Cuántos servidores Windows y Linux/Unix requerirían agente? ¿Son obligatorios desde la implementación inicial o pueden entregarse por fases?

El alcance estimado para el despliegue del agente es de alrededor de 110 servidores en total, distribuidos entre plataformas Windows y Linux/Unix, los cuales deben quedar completamente instalados y configurados dentro del plazo máximo de treinta (30) días calendario establecido para la implementación.

No es procedente la entrega por fases posteriores a dicho periodo, toda vez que el pago es único y se ejecutará contra la implementación y entrega a satisfacción de la totalidad de las licencias.

39. El requisito 12 del Anexo Técnico anuncia perfiles pero no contiene texto, y varios requisitos presentan errores de redacción (por ejemplo, 59, 71, 80 y 82). ¿Pueden publicar el anexo corregido?

Se eliminará el numeral 12 del Anexo Técnico, teniendo en cuenta que los perfiles del personal requerido ya se encuentran desarrollados posteriormente en el apartado “Perfiles Requeridos”, específicamente en los numerales 1. Gerente de Proyectos y 2. Especialista en Seguridad, donde se establecen su rol, formación académica, experiencia y certificaciones requeridas.

Adicionalmente, se corregirán los errores de redacción y numeración identificados en el Anexo Técnico y se publicará la versión ajustada del documento.

40. ¿La capacitación a los administradores y la entrega de manuales o documentación hacen parte del alcance? De ser así, ¿cuántas horas y personas se contemplan?

La Entidad aclara que la entrega de manuales y documentación técnica correspondiente a la solución hace parte de las condiciones necesarias para su implementación y operación.

En cuanto a la capacitación, los documentos del proceso no establecen una obligación independiente ni una intensidad horaria específica. No obstante, durante las actividades de implementación y puesta en marcha, el contratista deberá realizar el acompañamiento técnico necesario para que los administradores designados por la SCRД conozcan las funcionalidades y operación de la solución, de conformidad con el alcance definido en los documentos del proceso.





41. La cláusula décima quinta del contrato prohíbe subcontratar sin autorización previa y escrita. ¿Se autoriza que el soporte de las tecnologías integradas o parte

del equipo de trabajo sea provisto por aliados del contratista? ¿Cómo se solicitaría esa autorización?

Una vez revisado lo planteado por el observante y con el fin de precisar las condiciones aplicables a la ejecución del contrato, la Entidad modificará la Cláusula Décima Quinta – Cesión, estableciendo de manera expresa que no se permitirá la subcontratación de las actividades y obligaciones a cargo del contratista.

En consecuencia, dichas actividades deberán ser ejecutadas directamente por el contratista mediante el personal dispuesto y acreditado conforme a los requisitos establecidos en los documentos del proceso, siendo este el único responsable frente a la SCRD por el cumplimiento integral del objeto y de las obligaciones contractuales.

**42. ¿La implementación debe ser presencial o puede realizarse de forma remota?
¿Se requieren ambientes de pruebas y producción, y existen ventanas de mantenimiento definidas?**

La Entidad aclara que las actividades de implementación, parametrización, puesta en marcha y soporte de la solución PAM podrán realizarse de manera remota y/o presencial, de acuerdo con las necesidades técnicas que se presenten durante la ejecución y previa coordinación con el supervisor del contrato.

Frente a los ambientes de pruebas y producción, los documentos del proceso no establecen como requisito la disposición de ambientes independientes de pruebas y producción. La implementación deberá realizarse sobre los componentes y entornos tecnológicos que la SCRD determine y habilite para tal efecto, conforme con las especificaciones técnicas de la solución y en coordinación con el supervisor.

Así mismo, no se encuentran definidas previamente ventanas específicas de mantenimiento para la implementación. En caso de que las actividades a ejecutar requieran intervención sobre componentes tecnológicos en operación o puedan generar afectación a los servicios de la Entidad, las fechas y horarios correspondientes deberán ser previamente coordinados y autorizados por la SCRD, de acuerdo con sus procedimientos y necesidades operativas.

Respuesta a observaciones de Securesoft Colombia S.A.S.

Observación 1 – Numeral 7. Modalidad de despliegue de la solución SAPM



Solicitud:

Respetuosamente solicitamos modificar el numeral 7 para que se permita expresamente la presentación de soluciones bajo modalidad **SaaS administrada por el fabricante**, además de las modalidades actualmente contempladas, manteniendo para cualquiera de ellas el cumplimiento de las condiciones funcionales y de seguridad establecidas en el Anexo Técnico.

La Entidad no acepta la solicitud. Se mantienen las modalidades de despliegue establecidas en el Anexo Técnico, correspondientes a los factores de forma definidos para la solución PAM. En consecuencia, no se incorporará la modalidad SaaS administrada por el fabricante como alternativa adicional de despliegue.

Observación 2 – Numeral 10 – Herramientas de monitoreo de infraestructura

Solicitud: Respetuosamente solicitamos modificar el numeral 10 de manera que el requerimiento se concentre en el resultado esperado —contar con mecanismos para supervisar la disponibilidad, salud y operación de la solución PAM— y permita que dichas capacidades sean proporcionadas directamente por la plataforma o mediante integración con herramientas especializadas de monitoreo, **sin exigir que la solución PAM incorpore nativamente funcionalidades propias de herramientas como PRTG, MRTG o Cacti.**

La entidad modificará el numeral 10 del Anexo Técnico con el fin de alinear el requerimiento de monitoreo a las capacidades nativas de la solución PAM. El texto quedará redactado de la siguiente manera:

"10. Plataforma gráfica: Acceso web 7x24 a la consola de la solución PAM, que permita consultar en tiempo real e histórico la disponibilidad de sus componentes, el estado de las sesiones privilegiadas y demás indicadores relevantes del servicio a través de la misma solución"

Observación 3 – Numeral 11 – Certificación Common Criteria

Solicitud: Respetuosamente solicitamos modificar el numeral 11 permitiendo acreditar **al menos una (1) certificación Common Criteria del producto ofertado, en su versión actual o anterior**, o alternativamente aceptar certificaciones o evaluaciones independientes de seguridad reconocidas internacionalmente que permitan demostrar que la solución ha sido sometida a procesos formales de evaluación de sus controles de seguridad.

Se mantiene lo establecido en el anexo técnico del proceso, por lo cual los proponentes deben acreditar que la solución propuesta cuenta con al menos dos (2) certificaciones Common Criteria obtenidas de forma independiente correspondientes a versiones actuales y/o anteriores de la misma solución o producto ofertado. No es procedente reducir la exigencia a una sola certificación ni sustituirla por evaluaciones alternativas o equivalentes, ya que la entidad requiere garantizar de forma objetiva la continuidad en los controles de seguridad, la madurez en el ciclo de desarrollo y la robustez criptográfica de la plataforma unificada a lo largo del tiempo bajo estándares globales plenamente verificables.

Por lo anterior no se acepta la solicitud planteada por el observante.

Solicitud: Respetuosamente solicitamos modificar el numeral 13 para permitir que la solución garantice alta disponibilidad, redundancia y continuidad operativa mediante la arquitectura oficialmente diseñada y soportada por el fabricante, sin exigir específicamente una arquitectura activo-activo, replicación transaccional distribuida o base de datos embebida, y manteniendo como condición que la implementación no genere para la Entidad costos adicionales de licenciamiento de bases de datos que no hayan sido incluidos en la propuesta económica.

Se mantiene lo establecido en el numeral 13 del anexo técnico, por lo cual es obligatorio que la solución cuente de forma nativa con una arquitectura de clúster activo-activo, replicación transaccional distribuida y motor de base de datos embebido y endurecido de fábrica; no es procedente flexibilizar esta especificación a otros esquemas de alta disponibilidad que no aseguren la tolerancia a fallos inmediata y el balanceo de carga en tiempo real sin ventanas de conmutación, debiendo el proponente garantizar que el cumplimiento de esta arquitectura integral no genere costos adicionales de licenciamiento para la entidad.

Por lo anterior no se acepta la solicitud planteada por el observante.

Observación 5 al numeral 40 – Gestión de cuentas de servicio y dependencias de aplicaciones

Solicitud: Respetuosamente solicitamos modificar el numeral 40 eliminando la obligatoriedad específica de “reconfigurar automáticamente grupos de conexiones (connection pools) en servidores de aplicaciones sin generar desconexiones a usuarios finales”, y permitir que la actualización de las dependencias asociadas a las cuentas de servicio pueda realizarse mediante mecanismos nativos, conectores, APIs, scripts o integraciones oficialmente soportadas por la solución ofertada.

Se mantiene lo establecido en el numeral 40 del anexo técnico, toda vez que flexibilizar este requisito e incorporar el uso de scripts, APIs externas o conectores manuales introduce un riesgo crítico de inestabilidad



operativa, caídas de servicio y errores de autenticación en las aplicaciones y bases de datos institucionales de la entidad durante los ciclos de rotación de credenciales; por consiguiente, el proponente debe garantizar que la solución cuente con la capacidad nativa de reconfigurar automáticamente los grupos de conexiones (connection pools) asegurando la continuidad absoluta y la total transparencia para los usuarios finales.

Por lo anterior no se acepta la solicitud planteada por el observante.

Observación 6 – Numeral 43 – Protección de comunicaciones entre componentes

Solicitud: Respetuosamente solicitamos modificar el numeral 43 permitiendo que la protección de las comunicaciones pueda acreditarse mediante TLS/HTTPS, mTLS, certificados digitales, OAuth 2.0 u otros mecanismos criptográficos seguros y oficialmente soportados por el fabricante, siempre que permitan garantizar la confidencialidad e integridad de la información en tránsito y la autenticación de los componentes involucrados.

Se mantiene lo establecido en el numeral 43 del anexo técnico, por lo cual es obligatorio garantizar la autenticación mutua mediante certificados TLS (mTLS) en todas las comunicaciones internas de la solución. Flexibilizar este requisito hacia mecanismos simples como TLS estándar o tokens de autorización eleva el riesgo de ataques por suplantación de identidad de componentes (spoofing) e interceptación de tráfico, comprometiendo el aislamiento y la confianza de las credenciales de alta criticidad custodiadas en la bóveda central.

Por lo anterior no se acepta la solicitud planteada por el observante.

Observación 7 – Numeral 48 – Gestión segura de credenciales aplicación-a-aplicación

Solicitud: Respetuosamente solicitamos modificar el numeral 48 permitiendo que la solución proporcione mecanismos seguros para la autenticación aplicación-a-aplicación y la obtención dinámica de credenciales, secretos o tokens mediante **API REST, SDK, agentes, conectores, proxy u otros mecanismos equivalentes oficialmente soportados por el fabricante**, sin exigir específicamente la existencia de un proxy REST/SOAP intermedio ni establecer como condición absoluta que la integración se realice sin modificación alguna del código del sistema cliente.

Se mantiene lo establecido en el numeral 48 del anexo técnico, por lo cual la solución PAM debe proveer de forma obligatoria el proxy intermedio solicitado para interceptar, autenticar e inyectar de manera automatizada las credenciales sin alterar el código fuente de los sistemas existentes. Permitir modificaciones en el código de los sistemas clientes, incluso si son ejecutadas por el contratista, introduce riesgos críticos de pérdida de soporte y garantías de los fabricantes de las aplicaciones actuales (tales como Moodle o WordPress), genera dependencias complejas de mantenimiento para la entidad a futuro e imposibilita técnicamente el cumplimiento del plazo perentorio de treinta (30) días calendario establecido en los estudios previos para la implementación y entrega a satisfacción del proyecto.





Por lo anterior no se acepta la solicitud planteada por el observante.

Observación 8 – Numeral 52 - Distribución geográfica y acceso a secretos

Solicitud: Respetuosamente solicitamos modificar el numeral 52 permitiendo que la solución garantice el acceso seguro a secretos desde aplicaciones ubicadas en diferentes centros de datos, redes o ambientes de nube, mediante los mecanismos de distribución, conectividad, disponibilidad y arquitectura oficialmente soportados por el fabricante, sin exigir específicamente la sincronización automática de políticas de acceso entre nodos distribuidos geográficamente.

Se mantiene lo establecido en el numeral 52 del anexo técnico, por lo cual es obligatorio que la solución garantice la sincronización automática de políticas de acceso entre nodos distribuidos geográficamente. Flexibilizar este requisito hacia mecanismos de distribución generales del fabricante, sin sincronización automática y en tiempo real, introduce un riesgo crítico de inconsistencia en las políticas de seguridad, obligando a realizar tareas de replicación manual que comprometen la alta disponibilidad, la resiliencia y la continuidad operativa del ecosistema PAM ante contingencias entre el centro de datos principal y la nube de Azure.

Por lo anterior no se acepta la solicitud planteada por el observante.

Observación 9 – Numeral 58 – Indexación y búsqueda sobre sesiones privilegiadas

Solicitud: Respetuosamente solicitamos modificar el numeral 58 permitiendo que la solución proporcione capacidades de **consulta, búsqueda, reproducción y análisis de sesiones privilegiadas mediante OCR, metadatos, eventos de auditoría, registros o transcripciones de actividad, comandos u otros mecanismos equivalentes oficialmente soportados por el fabricante**, sin establecer el reconocimiento óptico de caracteres como mecanismo obligatorio.

Se aclara que el Reconocimiento Óptico de Caracteres (OCR) y el reconocimiento óptico son técnicamente el mismo componente tecnológico, por lo cual la entidad ratifica su carácter obligatorio y excluyente dentro del numeral 58 del anexo técnico. Eliminar la obligatoriedad de esta función para reemplazarla por metadatos o registros generales anularía la capacidad de indexar visualmente el texto en pantalla durante las sesiones gráficas (como RDP en Windows o plataformas Web), impidiendo realizar búsquedas inmediatas de palabras clave para saltar al segundo exacto del video.

Por lo anterior no se acepta la solicitud planteada por el observante.





Observación 10 – Numeral 59 - Prevención de exfiltración mediante portapapeles

Solicitud: Respetuosamente solicitamos modificar el numeral 59 permitiendo que la prevención de exfiltración mediante portapapeles pueda realizarse mediante **restricción, bloqueo, deshabilitación, inspección de contenido o mecanismos equivalentes de control del portapapeles**, sin establecer como obligatorio el análisis de cadenas y patrones estructurados ni el enmascaramiento dinámico de información.

Para la Entidad es un requisito crítico de seguridad no solo restringir de manera general el uso del portapapeles, sino contar con la capacidad técnica avanzada de identificar proactivamente datos regulados o sensibles mediante el análisis de cadenas y patrones estructurados, garantizando su protección o enmascaramiento sin irrumpir en la disponibilidad general de la herramienta.

Por lo anterior se mantiene lo establecido en el Anexo Técnico.

Observación 11 – Numeral 60 – Control de transferencia de archivos en sesiones privilegiadas

Solicitud: Respetuosamente solicitamos modificar el numeral 60 permitiendo que el control de transferencia de archivos durante sesiones privilegiadas pueda realizarse mediante mecanismos de **habilitación, restricción, autorización, bloqueo, inspección de contenido o controles equivalentes**, sin establecer como obligatorio que la plataforma PAM realice directamente análisis del contenido de los archivos transferidos.

Para la Entidad es un requisito crítico de seguridad garantizar que los archivos transferidos durante las sesiones de administración no contengan información clasificada o sensible en su interior. Limitar el control exclusivamente a la restricción de extensiones o parámetros generales resulta insuficiente frente a técnicas de evasión de seguridad. Por lo tanto, se mantiene la obligatoriedad de que la plataforma realice el análisis de contenido conforme a lo estipulado en el Anexo Técnico original.

Observación 12 – Numeral 73 – Control de operaciones sobre bases de datos



Solicitud: Respetuosamente solicitamos modificar el numeral 73 permitiendo que el control de operaciones críticas sobre bases de datos pueda realizarse mediante **restricción de acceso, políticas de autorización, control de privilegios, monitoreo y auditoría de actividad, control de comandos o sentencias cuando sea soportado, o mecanismos equivalentes**, sin establecer como obligatorio el bloqueo en tiempo real de sentencias DDL/DML destructivas por parte de la plataforma PAM.

Para la Entidad es un requisito indispensable mitigar en la fuente el riesgo de pérdida o alteración maliciosa de la información mediante errores o acciones no autorizadas de usuarios privilegiados. Limitar el control a una auditoría posterior al incidente resulta insuficiente para la protección de los activos de información críticos. Por lo tanto, se mantiene la obligatoriedad de que la solución realice el filtrado y bloqueo en tiempo real de sentencias destructivas conforme a lo establecido originalmente en el numeral 73 del Anexo Técnico.

Observación 13 – Numeral 77 – Autenticación reforzada para accesos privilegiados

Solicitud: Respetuosamente solicitamos modificar el numeral 77 permitiendo que la autenticación reforzada para sesiones privilegiadas de mayor riesgo pueda implementarse mediante **MFA, reautenticación/Step-up Authentication, políticas contextuales, flujos de aprobación u otros mecanismos de autenticación y autorización reforzada oficialmente soportados por el fabricante**, sin exigir específicamente un nuevo desafío MFA al inicio de cada sesión ni establecer como condición la verificación de presencia física del usuario frente al teclado.

La Entidad aclara que el objetivo fundamental es garantizar que quien inicia una sesión de alto riesgo sea efectivamente el usuario autorizado, mitigando ataques de secuestro de sesión. Reconociendo las mejores prácticas de la industria, se modifica el numeral 76 del Anexo Técnico, el cual quedará redactado de la siguiente manera:

"76. La solución debe contar con mecanismos de autenticación y autorización reforzada para sesiones privilegiadas de mayor riesgo, permitiendo la implementación de controles tales como Segundo Factor de Autenticación (MFA), re-autenticación/Step-up Authentication, aplicación de políticas contextuales, flujos de aprobación jerárquica u otros mecanismos equivalentes oficialmente soportados por el fabricante que aseguren la legitimidad del acceso."

Observación 14 – Numeral 87 – Prevención de movimiento lateral





Solicitud: Respetuosamente solicitamos modificar el numeral 87 permitiendo que la solución contribuya a prevenir o limitar el movimiento lateral asociado al compromiso o uso indebido de cuentas privilegiadas mediante **controles de acceso, mínimo privilegio, restricciones por políticas, acceso temporal o Just-in-Time, control de sesiones, microsegmentación u otros mecanismos equivalentes oficialmente soportados por el fabricante**, sin establecer como obligatoria la microsegmentación de comunicaciones de red a nivel de proceso o usuario.

Para la Entidad es un requerimiento técnico crítico contar con un control granular que restrinja las comunicaciones de red entrantes y salientes a nivel de procesos o usuarios en el host administrado, aislando de manera proactiva cualquier intento de tráfico lateral no autorizado.

Por lo anterior no se acepta la solicitud planteada por el observante.

Observación 15 general sobre los numerales 80 a 99 – Alcance funcional PAM y gestión de privilegios en endpoint



Por lo anterior, consideramos conveniente que la Entidad **aclare si dentro del alcance contractual se requiere adicionalmente una solución o módulo de Endpoint Privilege Management (EPM)**, incluyendo su correspondiente licenciamiento, implementación y dimensionamiento, o si el objeto del proceso corresponde principalmente a la implementación de una solución PAM.

En caso de que el alcance requerido corresponda exclusivamente a PAM, respetuosamente solicitamos revisar los numerales 80 a 99 y mantener como obligatorios únicamente aquellos requerimientos directamente relacionados con la administración y control de accesos privilegiados, permitiendo que las capacidades propias de EPM sean consideradas opcionales o complementarias.

En caso de que la Entidad confirme que EPM forma parte integral del alcance requerido, respetuosamente solicitamos **identificar expresamente dicho componente dentro de la arquitectura solicitada y establecer su dimensionamiento**, indicando como mínimo la cantidad de endpoints y/o servidores que deberán ser protegidos, sistemas operativos involucrados y demás condiciones necesarias para determinar correctamente el licenciamiento, implementación, soporte y costo de dicha solución.

Adicionalmente, teniendo en cuenta que el alcance inicial establece un licenciamiento de solución PAM para diez (10) usuarios, respetuosamente solicitamos aclarar cómo deberá dimensionarse y licenciarse el componente requerido para atender las funcionalidades de gestión de privilegios a nivel de endpoint/servidor establecidas en los numerales 80 a 99, indicando la cantidad de servidores, endpoints y sistemas operativos que deberán ser cubiertos.

La Entidad ratifica que las funcionalidades descritas en los numerales del 80 al 99 forman parte integral y obligatoria del alcance técnico requerido para este proceso. Las soluciones modernas de Gestión de Accesos Privilegiados (PAM) integran de forma nativa estas capacidades avanzadas de gestión de privilegios en el endpoint, control de comandos y protección a nivel de sistema operativo, las cuales son indispensables para mitigar los riesgos de seguridad en nuestra infraestructura crítica.

Con el fin de que los proponentes puedan realizar un correcto dimensionamiento, licenciamiento y costeo de estas capacidades modernas dentro de su propuesta económica, se aclara que el alcance del proyecto está definido para diez (10) usuarios administradores y un entorno compuesto por ciento diez (110) servidores que estarán integrados con la solución.



**Observación 16 general a los numerales 100 a 114 – Alcance de analítica avanzada de identidades e ITDR**

En consecuencia, respetuosamente solicitamos a la Entidad **aclarar si dentro del alcance contractual se requiere adicionalmente una solución o módulo especializado de ITDR/Identity Security Analytics**, además de la solución PAM solicitada.

En caso afirmativo, solicitamos que dicho componente sea identificado expresamente dentro de la arquitectura requerida y que se establezca su correspondiente alcance y dimensionamiento, incluyendo el total de las identidades, cuentas, activos, fuentes de información e integraciones que deberán ser cubiertas.

Teniendo en cuenta que el alcance inicial establece el licenciamiento de una solución PAM para diez (10) usuarios, respetuosamente solicitamos aclarar el dimensionamiento correspondiente a las capacidades de analítica avanzada de identidades requeridas en los numerales 100 a 114, indicando la cantidad total de identidades, cuentas de servicio, endpoints, servidores y activos de la Entidad, con el fin de que los oferentes puedan determinar de manera objetiva y comparable el licenciamiento y costo de la solución ofertada.

La Entidad aclara que no se requiere la adquisición ni el licenciamiento de una solución o módulo independiente o especializado de ITDR / Identity Security Analytics adicional a la solución PAM solicitada.

Las capacidades de analítica avanzada, comportamiento y algoritmos basadas en Machine Learning deben venir integradas dentro de la solución integral de PAM ofertada, sin que esto implique un licenciamiento por separado o un incremento en los módulos base.

Para efectos de un correcto y objetivo dimensionamiento y costeo de estas capacidades nativas por parte de los oferentes, se informa que el alcance del licenciamiento del PAM debe cubrir a los diez (10) usuarios administradores solicitados y alrededor de 110 servidores. Los proponentes deberán dimensionar sus ofertas integrales con base en estas métricas.

Observación 17 – Formación académica del Gerente de Proyecto

Solicitud: Respetuosamente solicitamos ampliar el requisito de formación académica permitiendo Especialización y/o Maestría en **Gerencia de Proyectos, Ingeniería de Software, Sistemas, Tecnologías de la Información, Seguridad de la Información o áreas afines**, siempre que el profesional acredite la experiencia en gestión de proyectos requerida por la Entidad.

La Entidad acoge la observación teniendo en cuenta las funciones asignadas al Gerente de Proyectos y con





el fin de ampliar la participación sin afectar la idoneidad requerida para la ejecución del contrato, se aceptará como formación de posgrado especialización y/o maestría en Gerencia de Proyectos, Dirección o Gestión de Proyectos, Ingeniería de Software, Sistemas, Tecnologías de la Información, Seguridad de la Información o áreas afines relacionadas con la gestión de proyectos tecnológicos.

En todo caso, el profesional deberá cumplir con los demás requisitos de formación, experiencia y certificaciones establecidos para el perfil en los documentos del proceso.

Por lo anterior, la Entidad realizará el ajuste correspondiente en los documentos del proceso.

Observación 18 – Certificación ITIL del Gerente de Proyecto

Solicitud: Respetuosamente solicitamos permitir la acreditación mediante **ITIL v3, ITIL v4 o certificación equivalente relacionada con gestión de servicios de tecnologías de información**, manteniendo los demás requisitos de experiencia y certificación establecidos para el perfil.

Para acreditar el requisito ITIL se aceptará ITIL v4 o ITIL 4 Foundation. No se aceptarán certificaciones correspondientes a versiones anteriores del marco ITIL. De acuerdo a lo anterior se realizará el ajuste correspondiente en el anexo técnico.

Los demás requisitos establecidos para el perfil se mantienen.

Respuesta a observaciones Empresa Grupo LUMA SAS

-"La solución ofertada debe como mínimo haber sido certificada dos (2) veces por la entidad Common Criteria para sus versiones actuales y/o anteriores..."

Se solicita amablemente a la entidad modificar el numeral de la siguiente manera: "La solución ofertada debe contar con certificación Common Criteria en su versión actual, O en su defecto, acreditar el cumplimiento del estándar FIPS 140-2 y/o certificaciones ISO 27001 / SOC2 en los procesos de desarrollo del fabricante." con el fin de no limitar la Participación de fabricantes con soluciones PAM.

Se mantiene lo establecido en el anexo técnico del proceso, por lo cual los proponentes deben acreditar que la solución propuesta cuenta con al menos dos (2) certificaciones Common Criteria obtenidas de forma independiente, correspondientes a versiones actuales y/o anteriores de la misma solución o producto ofertado. No es procedente reducir la exigencia a una sola certificación ni sustituirla por evaluaciones alternativas o equivalentes, ya que la entidad requiere garantizar de forma objetiva la continuidad en los controles de seguridad, la madurez en el ciclo de desarrollo y la robustez criptográfica de la plataforma unificada a lo largo del tiempo bajo estándares globales plenamente verificables.





-“La solución debe permitir una implementación modular de los controles... SAPM Shared Accounts Management, AAPM Application to Application Password Management, PSM SUPM...”

Se solicita amablemente a la entidad Ajustar la redacción para enfocarse en la funcionalidad y no en la arquitectura propietaria, de la siguiente manera: “La solución debe proveer capacidades nativas e integrales para la administración de cuentas compartidas, gestión de credenciales entre aplicaciones, y gestión de sesiones privilegiadas, ya sea mediante módulos independientes o como una plataforma unificada.”

Se aclara que los términos SAPM, AAPM, PSM y SUPM no corresponden a una arquitectura propietaria o exclusiva de un fabricante, sino que constituyen la taxonomía estándar e indicadores técnicos de referencia internacional para definir los pilares de una solución de Gestión de Accesos Privilegiados (PAM).

Por lo anterior no se acepta la solicitud planteada por el observante.

-“La solución debe contar con la capacidad de indexación por reconocimiento óptico de caracteres (OCR) sobre sesiones gráficas...”

se solicita amablemente a la entidad Ampliar el espectro tecnológico permitiendo alternativas equivalentes: “La solución debe contar con capacidades de búsqueda de auditoría sobre las sesiones mediante reconocimiento óptico de caracteres (OCR) O, de manera equivalente, mediante la indexación exhaustiva de comandos, captura de teclado (keystroke logging) y metadatos de la sesión.”

La entidad ratifica el carácter obligatorio y excluyente de la indexación por Reconocimiento Óptico de Caracteres (OCR) dentro del numeral 58 del Anexo Técnico.

Eliminar la obligatoriedad de esta funcionalidad para reemplazarla por metadatos, captura de teclado (keystroke logging) o registros generales de comandos anularía por completo la capacidad de indexar visualmente el texto en pantalla durante la ejecución de sesiones gráficas (tales como RDP en Windows o consolas Web).

Mantener este requisito es indispensable para la entidad, ya que es el único mecanismo tecnológico que garantiza al equipo de infraestructura la posibilidad de realizar búsquedas inmediatas de palabras clave dentro de entornos visuales y saltar al segundo exacto del video para realizar labores de soporte, revisión técnica y control forense.

Por lo anterior no se acepta la solicitud planteada por el observante.

-Se exigen módulos de kernel para restringir llamadas al sistema operativo (80, 82) y un motor de analítica basada en Machine Learning (100) para perfiles de comportamiento dentro del PAM

Se solicita amablemente a la entidad suprimir el requerimiento de intervención a nivel de kernel desde el agente PAM, o en su defecto, aclarar que: “Estas funcionalidades de protección de host, Machine Learning y análisis de comportamiento anómalo podrán ser suplidas de forma nativa por el PAM O mediante la integración nativa y certificada del PAM con las soluciones SIEM, EDR o consolas de analítica de seguridad con las que cuente la entidad o el fabricante propuesto.”

La entidad ratifica el carácter obligatorio y excluyente de los requisitos técnicos asociados al control por módulos de kernel (numerales 80 y 82) y al motor de analítica basada en Machine Learning (numerales 80, 82 y 100) de forma nativa dentro de la solución de PAM solicitada.

La exigencia de interceptar las llamadas al sistema operativo a nivel de kernel es indispensable para garantizar el principio de privilegio mínimo, impidiendo la elusión de controles de seguridad, la exfiltración de información a medios extraíbles y la alteración de archivos críticos (Tamper Protection), incluso por parte de usuarios con máximos privilegios administrativos. Permitir que estas funciones dependan de integraciones externas con soluciones tipo SIEM o EDR transferirá la carga operativa, el riesgo de desfase en la comunicación y los costos de licenciamiento de terceros a la entidad, desnaturalizando el alcance centralizado de control forense y mitigación en tiempo real que debe proveer la solución PAM.



Por lo anterior no se acepta la solicitud planteada por el observante.

Respuesta a observaciones Empresa RedNeet

OBSERVACIÓN # 1

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 9 (página 2):

9. La solución SAPM debe tener certificaciones tales como:

➤ **Validación de funcionamiento con FIPS 140-2.**

Solicitamos a la entidad modificar: el numeral 9, de manera que se acepte de forma indistinta la validación FIPS 140-2 o FIPS 140-3.

Lo anterior, teniendo en cuenta que el Programa de Validación de Módulos Criptográficos (CMVP) del NIST trasladó los certificados FIPS 140-2 a la lista histórica en septiembre de 2026, y que las nuevas validaciones se expiden únicamente bajo FIPS 140-3, estándar que sustituye al anterior. Exigir exclusivamente FIPS 140-2 favorece productos con validaciones antiguas y excluye soluciones validadas bajo el estándar vigente, en contravía de la **selección objetiva** y la **libre competencia**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

"9. La solución SAPM debe tener certificaciones tales como: Validación de funcionamiento con FIPS 140-2 o FIPS 140-3."

La Entidad acoge la solicitud y modificará el numeral 9 del Anexo Técnico con el fin de aceptar la validación bajo los estándares FIPS 140-2 o FIPS 140-3.

El alcance y la forma de acreditación de este requisito se precisarán en el Anexo Técnico ajustado.





OBSERVACIÓN # 2

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 4 (página 2):

4. La solución debe soportar los siguientes modos y entornos de trabajo en modo seguro:
- Modo: FIPS 140-2
 - Entorno: IPv4 y IPv6

Edificio ~~Ateliers~~: Calle 99 No. 12 – 39 Oficina 103
PBX: +57 (601) 2350962 Email: info@redneet.com
www.redneet.com Bogotá – Colombia.



Solicitamos a la entidad ajustar: el numeral 4, de manera que el modo seguro pueda operar bajo FIPS 140-2 o FIPS 140-3.

Lo anterior, teniendo en cuenta que FIPS 140-3 es el estándar vigente del NIST y mantener únicamente la versión anterior restringe la participación sin un beneficio técnico para la entidad, en contravía de la **libre concurrencia** y la **pluralidad de oferentes**.

En consistencia con la actualización tecnológica de los estándares criptográficos internacionales la entidad modificará el numeral 4 del Anexo Técnico.

OBSERVACIÓN # 3

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 11 (página 3):

11. La solución ofertada debe como mínimo haber sido certificada dos (2) veces por la entidad "Common Criteria" para sus versiones actuales y/o anteriores; esto con el fin de garantizar que el producto ofertado cumpla con las pruebas de Ciberseguridad más exigentes en el mercado por una entidad evaluadora independiente.

Solicitamos a la entidad flexibilizar: el numeral 11, de manera que se exija al menos una (1) certificación Common Criteria de la línea de producto ofertada.

Lo anterior, teniendo en cuenta que Common Criteria (ISO/IEC 15408) es un esquema internacional de evaluación y no una entidad certificadora, y que una sola certificación publicada en el portal oficial del esquema acredita la evaluación independiente que busca la entidad. Exigir dos certificaciones no aporta garantía técnica adicional y solo reduce el número de fabricantes elegibles, en contravía de la **selección objetiva** y la **libre concurrencia**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

"11. La solución ofertada debe contar como mínimo con una (1) certificación bajo el esquema Common Criteria (ISO/IEC 15408), verificable en el portal oficial del esquema, para su versión actual y/o versiones anteriores de la misma línea de producto."



Se mantiene lo establecido en el anexo técnico del proceso, por lo cual los proponentes deben acreditar que la solución propuesta cuenta con al menos dos (2) certificaciones Common Criteria obtenidas de forma independiente correspondientes a versiones actuales y/o anteriores de la misma solución o producto ofertado. No es procedente reducir la exigencia a una sola certificación.

Por lo anterior no se acepta la solicitud planteada por el observante.

OBSERVACIÓN # 4

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 10 (páginas 2 y 3):

10. Plataforma gráfica: Acceso web 7x24 a herramientas de consumo en tiempo real e histórico tipo:

PRTG, MRTG o Cacti o equivalente, que permita consultar como mínimo el consumo de ancho de banda en tiempo real e histórico, tráfico de entrada y salida, disponibilidad y demás indicadores relevantes del servicio.

Solicitamos a la entidad modificar: el numeral 10, de manera que se refiera a la consola de monitoreo propia de la solución PAM.

Lo anterior, teniendo en cuenta que las herramientas PRTG, MRTG y Cacti y los indicadores de ancho de banda y tráfico de entrada y salida corresponden a servicios de conectividad y no a una solución de gestión de accesos privilegiados. Mantener el requisito obligaría a cotizar una herramienta ajena al objeto y sin ítem en el presupuesto, en contravía de los principios de **planeación** y **economía**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

"10. Plataforma gráfica: Acceso web 7x24 a la consola de la solución PAM, que permita consultar en tiempo real e histórico la disponibilidad de sus componentes, el estado de las sesiones privilegiadas y demás indicadores relevantes del servicio."

Una vez revisada la observación, la Entidad aclara que se modificará el numeral 10 del Anexo Técnico, con el fin de alinear el requerimiento de monitoreo con las capacidades nativas de la solución PAM.

OBSERVACIÓN # 5

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 21 (páginas 3 y 4):

21. La solución debe tener la provisión de una bóveda centralizada con cifrado de grado militar (AES-256 o superior) para la custodia de credenciales, donde las llaves maestras de cifrado residan exclusivamente en un módulo HSM.

Solicitamos a la entidad ajustar: el numeral 21, de manera que el HSM sea una capacidad de integración y no un elemento de suministro obligatorio, o en su defecto aclarar si la entidad cuenta con un HSM propio.

Lo anterior, teniendo en cuenta que el cuadro de cantidades no incluye un módulo HSM físico ni en la nube, que su costo puede representar una parte relevante del presupuesto, y que las soluciones en appliance virtual protegen la llave maestra mediante módulos criptográficos validados FIPS. Exigir un HSM sin presupuestarlo afecta la **planeación** y el **equilibrio económico** del contrato.



La entidad ratifica la obligatoriedad de que las llaves maestras de cifrado residan exclusivamente en un módulo HSM, tal como lo exige el Anexo Técnico.

Desde el punto de vista de arquitectura de seguridad y el modelo Zero Trust, el uso de un HSM no es un elemento opcional de integración, sino un control crítico de segregación de funciones criptográficas. Permitir que la llave maestra resida en el mismo entorno lógico o disco del appliance virtual (aun estando validada por FIPS) expone al sistema a riesgos de exfiltración de memoria o compromisos del hipervisor por parte de administradores con privilegios elevados. El HSM garantiza que la llave de cifrado principal nunca sea expuesta en texto claro fuera del módulo HSM.

Respecto del suministro y costos asociados, se precisa que la solución deberá contar con la capacidad, conectores, licencias y configuraciones necesarias para operar con el HSM requerido. Dichos componentes propios de la solución deberán estar incluidos dentro de la propuesta económica del oferente.

La entidad no cuenta con un HSM, por lo anterior no se acepta la solicitud planteada por el observante.

OBSERVACIÓN # 6

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 7 (página 2):

7. La solución SAPM debe poder ser provista en los siguientes factores de forma:

- Virtual Appliance (VMware, OVA, KVM)
- En la nube (Azure: Nube de Microsoft en formato VHD)

Este despliegue debe contemplar adicionalmente lo siguiente:

- Híbrido, una parte On-Premise y su replicación en nube
- No requerir de motores de base de datos
- No requerir de sistemas operativos

Solicitamos a la entidad aclarar: (i) si el despliegue híbrido con replicación en Azure debe implementarse dentro del contrato o si se trata de una capacidad que la solución debe soportar; (ii) si la entidad cuenta con suscripción (tenant) de Azure y asume los costos de consumo de la infraestructura en nube; y (iii) qué recursos de virtualización on-premise (hipervisor, vCPU, memoria RAM y almacenamiento) pondrá a disposición la entidad.

Lo anterior, teniendo en cuenta que el cuadro de cantidades no incluye infraestructura de nube ni de cómputo, y que sin esta precisión los oferentes no pueden costear el mismo alcance, en contravía de la igualdad de oferentes y la selección objetiva.

La entidad se permite precisar que cuenta con suscripción (tenant) propia de nube pública en Azure, así como con infraestructura propia On-Premise.

El requerimiento técnico corresponde a una capacidad que la solución ofertada debe soportar de forma nativa en cualquiera de los dos entornos, permitiendo que la entidad elija la modalidad de despliegue (nube, local o híbrida) que mejor se adapte a sus necesidades durante la ejecución del contrato. La entidad asumirá

directamente los costos de consumo de su infraestructura y de la nube de Azure, por lo que el oferente no debe incluir dichos costos en su propuesta económica. Los recursos de virtualización específicos se dimensionarán de mutuo acuerdo con el contratista seleccionado durante la fase de planeación de la implementación.

OBSERVACIÓN # 7

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 2 (páginas 1 y 2):

2. La solución debe permitir soportar al menos los siguientes sistemas objetivos:

- Servidores Windows
- Servidores UNIX/LINUX
- Servidores ORACLE
- Mainframes IBM
- Dispositivos de red
- Servicios en la nube
- Plataformas WEB de diferentes Fabricantes

Edificio Ateliers: Calle 99 No. 12 – 39 Oficina 103
PBX: +57 (601) 2350962 Email: info@redneet.com
www.redneet.com Bogotá – Colombia.



Solicitamos a la entidad modificar: el numeral 2, eliminando los Mainframes IBM como sistema objetivo, salvo que la entidad cuente con este tipo de plataforma en su infraestructura.

Lo anterior, teniendo en cuenta que el soporte a mainframe es una capacidad de nicho ofrecida por un número reducido de fabricantes, y que su exigencia sin que exista en la infraestructura de la SCRD restringe la participación sin aportar valor al objeto, en contravía de la **planeación** y la **libre competencia**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

La entidad se permite precisar que actualmente no cuenta con la plataforma Mainframe IBM en operación dentro de su infraestructura tecnológica.

Sin embargo, la solución PAM ofrecida debe cumplir de forma obligatoria con la capacidad técnica nativa de



soportar dicha plataforma a futuro, conforme a lo solicitado en el numeral 2 del Anexo Técnico, con el fin de garantizar la escalabilidad y proyección tecnológica de la entidad. Por consiguiente, se mantiene la obligatoriedad del requerimiento y la redacción original del numeral 2.

Por lo anterior no se acepta la solicitud planteada por el observante.

OBSERVACIÓN # 8

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 87 (página 9):

87. La solución debe realizar la microsegmentación basada en host que restrinja las comunicaciones de red entrantes y salientes a nivel de proceso o usuario específico, bloqueando el tráfico lateral no autorizado de cuentas comprometidas.

Solicitamos a la entidad modificar: el numeral 87, de manera que esta capacidad pueda cumplirse de forma nativa o mediante integración con las plataformas de seguridad de endpoint o de red existentes en la entidad.

Lo anterior, teniendo en cuenta que la microsegmentación de red es una función propia de plataformas de firewall de host, EDR/XDR o microsegmentación, y no de la gestión de accesos privilegiados. Exigirla de forma nativa en el PAM limita el mercado a muy pocos fabricantes, en contravía de la **libre concurrencia** y la **selección objetiva**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

*"87. La solución debe realizar **de forma nativa o mediante integración con las plataformas EDR/XDR o de firewall existentes en la entidad** la microsegmentación basada en host que restrinja las comunicaciones de red entrantes y salientes, bloqueando el tráfico lateral no autorizado de cuentas comprometidas."*

La entidad ratifica el carácter obligatorio y excluyente de la capacidad de realizar microsegmentación basada en host de forma nativa dentro de la solución de PAM, tal como lo exige el numeral 87 del Anexo Técnico.

Permitir que esta función dependa de integraciones con plataformas externas (como EDR/XDR o firewalls de terceros existentes en la entidad) introduciría dependencias de configuración y afectaría el alcance de control centralizado requerido por la entidad. Por consiguiente, se mantiene la redacción original del numeral 87.

Por lo anterior no se acepta la solicitud planteada por el observante.

OBSERVACIÓN # 9

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 90 (página 9):

- 90.** La solución debe contar con reglas de confinamiento (Sandboxing) para aplicaciones vulnerables expuestas a internet, limitando estrictamente el alcance de los procesos comprometidos y evitando que afecten el sistema operativo subyacente.

edificio Ateliers: Calle 99 No. 12 – 39 Oficina 103
BX: +57 (601) 2350962 Email: info@redneet.com
www.redneet.com Bogotá – Colombia.



Solicitamos a la entidad modificar: el numeral 90, de manera que el confinamiento pueda cumplirse de forma nativa o mediante integración con la plataforma de protección de endpoint de la entidad.

Lo anterior, teniendo en cuenta que el sandboxing de aplicaciones expuestas a internet es una función de protección de servidores (HIPS/EDR), ajena al control de accesos privilegiados objeto del proceso, y su exigencia nativa restringe la **pluralidad de oferentes**.

La entidad ratifica el carácter obligatorio y excluyente de contar con reglas de confinamiento (Sandboxing) de forma nativa dentro de la solución de PAM, tal como lo exige el numeral 90 del Anexo Técnico.

Permitir que esta función dependa de integraciones con plataformas externas de protección de endpoint introduciría dependencias de configuración ajenas a la plataforma y afectaría el alcance de control y aislamiento inmediato requerido por la entidad para las aplicaciones expuestas.

Por lo anterior no se acepta la solicitud planteada por el observante.



OBSERVACIÓN # 10

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 98 (página 10):

98. La solución debe tener la capacidad de aplicar políticas de aislamiento lógico de tenants y aplicaciones dentro de un mismo sistema operativo, evitando que procesos de una unidad de negocio accedan a la memoria de otra.

Solicitamos a la entidad modificar: el numeral 98, eliminando el aislamiento de memoria entre procesos de distintas unidades de negocio, o en su defecto aclarar qué escenario de la SCRD exige esta capacidad.

Lo anterior, teniendo en cuenta que la SCRD es una sola entidad sin unidades de negocio multi-tenant sobre un mismo sistema operativo, y que el aislamiento de memoria entre procesos es una función del sistema operativo o de plataformas de control de aplicaciones, no del PAM. Su exigencia no guarda relación con la necesidad y afecta el principio de **planeación**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

*"98. La solución debe tener la capacidad de aplicar políticas **de control de acceso por grupo, rol o dependencia sobre las cuentas y activos gestionados.**"*

Si bien la Secretaría Distrital de Cultura, Recreación y Deporte (SCRD) es una única entidad, su infraestructura tecnológica alberga múltiples plataformas institucionales, sistemas misionales y portales ciudadanos que operan de forma simultánea. La exigencia de aislamiento lógico y control de acceso a la memoria entre procesos busca evitar que el compromiso o la explotación de una vulnerabilidad en una aplicación expuesta permita a un atacante o a un administrador con privilegios delegados realizar inyección de código o lectura directa de memoria hacia los procesos de otra aplicación crítica que cohabiten en el mismo sistema operativo.

OBSERVACIÓN # 11

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el cuadro "Servicio de gestión de accesos privilegiados (PAM)" (página 1):

Servicio de gestión de accesos privilegiados (PAM)	Cantidad
Adquisición del licenciamiento en suscripción de la solución de PAM por usuario por 12 meses.	10
Implementación, puesta en marcha y parametrización de la solución de PAM	1
Profesional certificado en soluciones de Gestión de Acceso Privilegiados (PAM) a implementar	1
Gerente de Proyectos para liderar la planificación, el seguimiento y la ejecución del proyecto.	1
Bolsa de horas de soporte	50

Solicitamos a la entidad aclarar: (i) si los diez (10) usuarios corresponden a administradores privilegiados nominados o concurrentes; (ii) la cantidad de activos objetivo a gestionar (servidores Windows, servidores Unix/Linux, bases de datos, dispositivos de red, consolas de nube y aplicaciones web); (iii) la cantidad de servidores en los que deben desplegarse los controles a nivel de sistema operativo de los numerales 80 a 99; (iv) la cantidad de aplicaciones o secretos a gestionar con el módulo AAPM; y (v) si las diez licencias deben cubrir la totalidad de los módulos SAPM, AAPM, PSM, SUPM y analítica de comportamiento.

Lo anterior, teniendo en cuenta que los fabricantes PAM licencian con métricas distintas (por usuario, por activo, por servidor con agente o por aplicación), y que sin el inventario de la entidad cada oferente dimensionará un alcance diferente, lo que impide comparar ofertas en igualdad de condiciones en una subasta por precio, en contravía de la **igualdad de oferentes**, la **selección objetiva** y las **reglas claras, justas y completas**.

La entidad se permite precisar de manera puntual las cinco (5) consultas realizadas por el proponente, con el fin de unificar el criterio de dimensionamiento económico:

- (i) Respecto a los diez (10) usuarios: Se aclara que corresponden a diez (10) usuarios administradores nominados (personal técnico de la oficina de TI), quienes utilizarán la plataforma PAM de manera directa para establecer sus conexiones seguras.
- (ii) Respecto a la cantidad de activos objetivo: Se precisa que la solución PAM gestionará un inventario inicial estimado de ciento diez (110) servidores distribuidos entre entornos Windows y Linux.
- (iii) Respecto a los servidores para despliegue de controles (numerales 80 a 99): El oferente debe dimensionar el alcance para la totalidad de los activos objetivo descritos en el punto anterior (110 servidores Windows y Linux), donde se aplicarán las políticas avanzadas de control y protección a nivel de sistema operativo.



(iv) Respecto a la cantidad de aplicaciones o secretos (módulo AAPM): Para efectos de la propuesta económica y técnica, el proponente debe incluir la capacidad de gestionar los secretos y llaves asociadas a la administración de los 110 servidores de la infraestructura tecnológica indicada.

(v) Respecto a la cobertura de las diez (10) licencias: Se confirma que las licencias y la solución PAM ofertada debe cubrir la totalidad de las capacidades solicitadas en el anexo técnico: los módulos SAPM, AAPM, PSM, SUPM y analítica de comportamiento

OBSERVACION # 12

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 7 (página 2):

7. La solución SAPM debe poder ser provista en los siguientes factores de forma:

- Virtual Appliance (VMware, OVA, KVM)
- En la nube (Azure: Nube de Microsoft en formato VHD)

Este despliegue debe contemplar adicionalmente lo siguiente:

- Híbrido, una parte On-Premise y su replicación en nube
- No requerir de motores de base de datos
- No requerir de sistemas operativos

Edificio Ateliers: Calle 99 No. 12 – 39 Oficina 103
PBX: +57 (601) 2350962 Email: info@redneet.com
www.redneet.com Bogotá – Colombia.



Solicitamos a la entidad flexibilizar: las condiciones "No requerir de motores de base de datos" y "No requerir de sistemas operativos", de manera que se acepten también soluciones desplegadas en máquina virtual cuyo sistema operativo y motor de base de datos estén incluidos en la solución o sean de licenciamiento libre, sin costo adicional de licenciamiento para la entidad.

Lo anterior, teniendo en cuenta que la finalidad del requisito es que la entidad no asuma licenciamiento adicional de sistemas operativos o bases de datos, finalidad que se cumple igualmente con soluciones que incorporan una base de datos embebida y se instalan sobre sistemas operativos de libre uso o incluidos. La exigencia exclusiva de un appliance cerrado limita la participación a pocos fabricantes, en contravía de la **libre concurrencia** y la **pluralidad de oferentes**.



La exigencia de estas condiciones responde estrictamente a motivos de seguridad de la información y endurecimiento de la infraestructura (Hardening). La solución solicitada debe operar bajo el modelo de Appliance Virtual Cerrado o Sólido, donde el sistema operativo y el motor de almacenamiento de datos se encuentren embebidos, sellados y protegidos de fábrica por el fabricante.

Permitir el despliegue sobre sistemas operativos o bases de datos genéricas administrables por fuera del ciclo de vida del Appliance incrementaría la superficie de ataque de la plataforma PAM, expondría la solución a vulnerabilidades lógicas y obligaría a la entidad a asumir tareas de gestión de parches, mantenimiento y aseguramiento de componentes externos a la aplicación de seguridad. Con el fin de mitigar riesgos criptográficos y de acceso a la bóveda centralizada, se mantiene la redacción original del numeral 7.

Por lo anterior no se acepta la solicitud planteada por el observante.

OBSERVACIÓN # 13

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 13 (página 3):

- 13. La solución debe incorporar una arquitectura de clúster activo-activo con replicación transaccional distribuida y base de datos embebida endurecida, garantizando disponibilidad continua sin requerir licenciamiento de bases de datos externas.**

Solicitamos a la entidad flexibilizar: el numeral 13, de manera que se acepte una arquitectura de alta disponibilidad activo-activo o activo-pasivo con replicación de la base de datos, siempre que esta se encuentre incluida en la solución.

Lo anterior, teniendo en cuenta que el objetivo de disponibilidad continua sin licenciamiento de bases de datos externas se alcanza con distintas arquitecturas de alta disponibilidad, y que exigir un esquema de clúster particular describe la implementación de un fabricante específico, en contravía de la **selección objetiva** y la **libre competencia**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

*"13. La solución debe incorporar una arquitectura de **alta disponibilidad (activo-activo o activo-pasivo)** con replicación **de la base de datos incluida en la solución**, garantizando disponibilidad continua sin requerir licenciamiento de bases de datos externas."*

De acuerdo con lo establecido en el anexo técnico, la solución debe contar de forma nativa con una arquitectura de clúster activo-activo con replicación transaccional distribuida. No es procedente la adopción de un esquema activo-pasivo, ya que la entidad requiere garantizar la alta disponibilidad simultánea, el balanceo de carga en tiempo real y la tolerancia a fallos inmediatos sin tiempos de espera ni ventanas de conmutación para la operación de la plataforma PAM.

Por lo anterior no se acepta la solicitud planteada por el observante.

**OBSERVACIÓN # 14**

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 80 (página 8):

80. La solución debe contar con la capacidad de aplicar controles de acceso obligatorios basados en módulos de kernel en servidores Linux/Unix/Windows, interceptando llamadas al sistema para gobernar qué procesos, archivos y puertos puede manipular un administrador.

Solicitamos a la entidad modificar: los numerales 80 a 99, correspondientes al control de superusuarios a nivel de sistema operativo (SUPM), de manera que sean calificados como deseables u opcionales y no como requisitos mínimos habilitantes.

Lo anterior, teniendo en cuenta que estos veinte (20) numerales describen controles a nivel de kernel (interceptación de llamadas al sistema, protección de integridad de archivos, control de ejecución de binarios, protección del registro de Windows, entre otros) propios de plataformas de protección de servidores, que no hacen parte del núcleo de una solución de gestión de accesos privilegiados, no están dimensionados en el cuadro de cantidades y difícilmente pueden desplegarse en servidores productivos dentro de un plazo de treinta (30) días. Su exigencia como requisito mínimo restringe el mercado a muy pocos fabricantes, en contravía de la **libre concurrencia**, la **proporcionalidad** y la **planeación**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

"Los numerales 80 a 99 se consideran funcionalidades deseables. Su no ofrecimiento no será causal de rechazo ni de no habilitación técnica de la oferta."

La Entidad ratifica que las funcionalidades descritas en los numerales del 80 al 99 forman parte integral y obligatoria del alcance técnico requerido para este proceso. Las soluciones modernas de Gestión de Accesos Privilegiados (PAM) integran de forma nativa estas capacidades avanzadas de gestión de privilegios en el endpoint, control de comandos y protección a nivel de sistema operativo, las cuales son indispensables para mitigar los riesgos de seguridad en nuestra infraestructura crítica.

Por lo anterior no se acepta la solicitud planteada por el observante.



OBSERVACIÓN # 15

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 100 (página 10):

100. La solución debe contar con un motor de analítica basada en Machine Learning que construye perfiles de comportamiento basal por administrador y detecta patrones anómalos, tales como horarios inusuales, secuencias atípicas o acceso a recursos no habituales.

Solicitamos a la entidad modificar: los numerales 100 a 114, correspondientes a analítica de comportamiento, de manera que puedan cumplirse de forma nativa o mediante integración con plataformas SIEM/UEBA del mismo fabricante o de la entidad, o en su defecto que sean calificados como deseables.

Lo anterior, teniendo en cuenta que la analítica de comportamiento con aprendizaje automático es provista por los fabricantes en módulos o plataformas complementarias, y que los modelos de comportamiento requieren un periodo de aprendizaje superior al plazo de ejecución del contrato. Exigirla como capacidad nativa del PAM restringe la **pluralidad de oferentes** sin beneficio funcional adicional, en contravía de la **selección objetiva**.

La entidad ratifica el carácter obligatorio y excluyente de las capacidades analíticas basadas en Machine Learning de forma nativa dentro de la solución de PAM, de conformidad con lo exigido en los numerales 100 a 114 del Anexo Técnico.

Permitir que esta funcionalidad dependa de integraciones externas con plataformas tipo SIEM o UEBA ajenas a la solución introduciría latencias operativas y complejidades técnicas que afectarían la capacidad de la plataforma para detectar patrones anómalos y ejecutar acciones de contención automáticas en tiempo real sobre las sesiones privilegiadas. Las capacidades nativas de analítica de comportamiento son indispensables para garantizar el control forense inmediato requerido por la entidad.

Por lo anterior no se acepta la solicitud planteada por el observante.



OBSERVACIÓN # 16

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 64 (página 7):

- 64.** La solución debe realizar el aislamiento de sesiones web para consolas de nube (AWS, Azure, Portales SaaS) en un navegador virtualizado y efímero, inyectando credenciales y restringiendo la descarga de artefactos o visibilidad de secretos.

Solicitamos a la entidad modificar: el numeral 64, de manera que el aislamiento de sesiones web en navegador virtualizado sea calificado como deseable, aceptando como mínimo el acceso intermediado y grabado a las consolas de nube con inyección de credenciales.

Lo anterior, teniendo en cuenta que el aislamiento en navegador virtualizado y efímero es una funcionalidad específica de pocas soluciones del mercado, mientras que el objetivo de control (que el operador no conozca la credencial y que la sesión quede auditada) se cumple con el acceso intermediado e inyección de credenciales, en contravía de la **libre concurrencia**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

*"64. La solución debe realizar **el acceso intermediado y grabado** a consolas de nube (AWS, Azure, Portales SaaS), inyectando credenciales y restringiendo la visibilidad de secretos. **El aislamiento en navegador virtualizado y efímero se considera una funcionalidad deseable.**"*

La entidad ratifica el carácter obligatorio y excluyente del aislamiento de sesiones web mediante navegador virtualizado y efímero, tal como lo exige el numeral 64 del Anexo Técnico.

Permitir que esta función se reduzca a una condición deseable o se reemplace por un acceso intermediado tradicional comprometería la seguridad de los entornos de nube. El navegador virtualizado y efímero es el único mecanismo técnico que garantiza la contención frente a riesgos de robo de cookies de sesión, inyección de scripts maliciosos o almacenamiento involuntario de artefactos técnicos en el endpoint del operador, por lo cual se mantiene la redacción original del numeral 64.



OBSERVACIÓN # 17

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 11 (página 3):

- 11. La solución ofertada debe como mínimo haber sido certificada dos (2) veces por la entidad "Common Criteria" para sus versiones actuales y/o anteriores; esto con el fin de garantizar que el producto ofertado cumpla con las pruebas de Ciberseguridad más exigentes en el mercado por una entidad evaluadora independiente.**

Solicitamos a la entidad flexibilizar: el numeral 11, de manera que, en caso de no acogerse la observación sobre una única certificación Common Criteria, se acepten de forma alternativa otras evaluaciones de seguridad independientes y verificables del fabricante o del producto.

Lo anterior, teniendo en cuenta que la finalidad declarada por la entidad es que el producto haya sido evaluado por un tercero independiente, finalidad que también cumplen certificaciones como ISO/IEC

Edificio Ateliers: Calle 99 No. 12 – 39 Oficina 103
PBX: +57 (601) 2350962 Email: info@redneet.com
www.redneet.com Bogotá – Colombia.



27001 del fabricante, informes SOC 2 Tipo II o pruebas de penetración independientes, en garantía de la **libre concurrencia** y la **pluralidad de oferentes**.

Por lo tanto, sugerimos dejar el requerimiento de la siguiente forma:

La Entidad no acoge la solicitud y mantiene la exigencia de las dos (2) certificaciones Common Criteria establecidas en el numeral 11 del Anexo Técnico. Las certificaciones ISO/IEC 27001, SOC 2 Tipo II u otras certificaciones organizacionales no sustituyen el requisito Common Criteria establecido para la solución ofertada.

En consecuencia, se mantiene la condición prevista en los documentos del proceso.



OBSERVACIÓN # 18

De acuerdo con el documento "ANEXO DE ESPECIFICACIONES TÉCNICAS", la entidad menciona lo siguiente en el numeral 9 (página 2):

9. La solución SAPM debe tener certificaciones tales como:

➤ **Validación de funcionamiento con FIPS 140-2.**

Solicitamos a la entidad aclarar: si la "validación de funcionamiento con FIPS 140-2" se acredita con la operación de la solución en modo conforme a FIPS, utilizando módulos o librerías criptográficas validadas, o si se exige que el producto ofertado cuente con un certificado CMVP propio.

Lo anterior, teniendo en cuenta que la expresión "validación de funcionamiento" admite ambas interpretaciones y que muchas soluciones del mercado operan en modo FIPS mediante módulos criptográficos validados de terceros, por lo que la precisión es necesaria para la **selección objetiva** y la **seguridad jurídica** de la verificación técnica.

La Entidad aclara que la "validación de funcionamiento con FIPS" se entenderá cumplida cuando la solución ofertada opere utilizando módulos criptográficos validados bajo los estándares FIPS 140-2 o FIPS 140-3, cuya validación pueda ser verificada mediante la documentación o fuente oficial correspondiente.

En consecuencia, no se exigirá que la solución PAM cuente con un certificado CMVP propio, siempre que los módulos criptográficos utilizados para su operación se encuentren debidamente validados bajo alguno de los estándares señalados.

De acuerdo con lo anterior, la Entidad realizará el ajuste correspondiente en el Anexo Técnico con el fin de precisar el alcance del requisito.



OBSERVACIÓN # 19

La entidad menciona lo siguiente:

Formación Académica: Título profesional en Ingeniería de Sistemas, Ingeniería de Computación, Ingeniería de Telecomunicaciones o carreras afines (reconocidas conforme al SNIES).
Especialización y/o Maestría en Gerencia de Proyectos.

Solicitamos a la Entidad considerar la inclusión de la **Especialización en Gerencia de Tecnología** dentro de las alternativas de formación posgradual aceptadas para el perfil requerido.

Lo anterior, teniendo en cuenta que dicha especialización presenta una **relación directa y pertinente con el componente de gerencia exigido por la Entidad**, toda vez que su formación integra conocimientos y competencias asociados con la planeación, dirección, gestión y toma de decisiones en entornos tecnológicos, aspectos que guardan correspondencia con el propósito y las responsabilidades previstas para el perfil solicitado.

Adicionalmente, de acuerdo con la clasificación y naturaleza académica registrada en el **Sistema Nacional de Información de la Educación Superior – SNIES**, este programa desarrolla competencias afines al campo de la gerencia y la gestión, por lo que su inclusión permitiría reconocer perfiles profesionales que cuentan con formación

edificio **Ateliers**: Calle 99 No. 12 – 39 Oficina 103
BX: +57 (601) 2350962 Email: info@redneet.com
www.redneet.com Bogotá – Colombia.



idónea y directamente relacionada con las funciones a desempeñar, **sin afectar ni disminuir las condiciones técnicas o académicas establecidas por la Entidad.**

La Entidad acoge parcialmente la observación.

Teniendo en cuenta las funciones asignadas al Gerente de Proyectos y con el fin de ampliar la participación sin afectar la idoneidad requerida para la ejecución del contrato, se aceptará como formación de posgrado especialización y/o maestría en Gerencia de Proyectos, Dirección o Gestión de Proyectos, Ingeniería de Software, Sistemas, Tecnologías de la Información, Seguridad de la Información o áreas afines relacionadas con la gestión de proyectos tecnológicos.

En todo caso, el profesional deberá cumplir con los demás requisitos de formación, experiencia y



certificaciones establecidos para el perfil en los documentos del proceso.

Por lo anterior, la Entidad realizará el ajuste correspondiente en los documentos del proceso.

Documento 20261600600893 firmado electrónicamente por:	
Javier Enrique Mariño Navarro	Jefe Oficina de Tecnologías de la Información Oficina de Tecnologías de la Información Fecha firma: 14-10-2026 17:40:47
Catherine Andrea Arias Torres	Contratista Oficina de Tecnologías de la Información Fecha firma: 14-10-2026 17:40:00
Ivan Esteban Lozano Aguilar	Contratista Oficina de Tecnologías de la Información Fecha firma: 15-10-2026 08:48:59
 e2be6c7305d9718d847b2aae2885809ce5f1318f041a2ac5e079893b186fa9d8 Codigo de Verificación CV: 393e5	