ADENDA No. 01
Invitación Abierta 005-2023

En consideración al proceso de Invitación abierta No. 005-2023 el cual tiene por objeto "EL PROVEEDOR se compromete con LA PREVISORA S.A. a realizar la implementación de una solución que permita la administración, identificación, detección, protección y respuesta frente a posibles brechas de seguridad a nivel de fuga de información DLP.", la Gerencia de TI de **LA PREVISORA S.A.**, realiza la siguiente modificación al documento de condiciones definitivas de la mencionada invitación.

1. Se modifica el numeral **17. Cronograma del proceso de la INFORMACION GENERAL del capítulo I del documento de condiciones,** el cual quedará de la siguiente manera expresado en color rojo:

17. Cronograma del proceso

ACTIVIDAD	PLAZO
Publicación del documento de condiciones definitivas en la página Web y apertura del proceso de contratación.	**24 de febrero 2023**
Plazo para presentar observaciones y preguntas con relación al documento de condiciones definitivas	**01 de marzo 2023 hasta las 5:00pm**
Respuestas de observaciones y preguntas con relación al documento de condiciones definitivas	**07 de marzo 2023**
Entrega de propuestas	**14 de marzo 2023** **A partir de las 07:00:00 am y hasta la 1:00:00 pm, vía correo electrónico**
Audiencia de Cierre de la invitación abierta	**14 de marzo 2023 a las 4:00 pm mediante evento en vivo en la herramienta Microsoft Teams.**
Término para evaluación y recibo de documentos de aclaraciones solicitadas	**17 de marzo 2023**
Publicación del Informe de requisitos habilitantes y el informe de evaluación	**22 de marzo 2023**
Recibo de observaciones a las evaluaciones	**24 de marzo 2023**
Resultado del proceso	**27 de marzo 2023**

2. Se modifica el numeral **3. De orden técnico (Capacidad técnica) ítem b. Condiciones técnicas obligatorias de los ASPECTOS HABILITANTES del capítulo III del documento de condiciones,** el cual quedará de la siguiente manera expresado en color rojo:

b. Condiciones técnicas obligatorias.

Todos los servicios y requerimientos descritos en el presente numeral son de obligatorio cumplimiento para la prestación del servicio, las propuestas que no cumplan con la totalidad de los requerimientos, no se tendrán en cuenta en el proceso de selección, por lo tanto, no serán calificadas.

LOS OFERENTES aceptan íntegramente las condiciones y obligaciones establecidas en esta invitación, la cual formará parte integral del contrato a celebrar.

Se debe indicar de manera expresa por parte de **EL OFERENTE** en su propuesta, una manifestación sobre su cumplimiento (cumple/no cumple) para cada uno de los siguientes requerimientos técnicos ANEXO REQUISITOS TECNOLOGICOS MINIMOS:

1. La plataforma debe proveerse como un servicio SaaS
2. Se solicita efectuar todas las fases de implementación DLP descritas por Gartner, en las que se genere el alcance, la concientización, se estructure el diseño, se aborden las dependencias y finalmente se implemente opere y evolucione la solución.
3. La solución debe contar con una consola centralizada, adicionalmente no solo se debe centrar en las soluciones de office365 (e-mail actual), sino que debe validar todo el tráfico que cursa sobre la red y la web en general.
4. La solución debe brindar el monitoreo de extremo a extremo y garantizar que esta solución no afecte el rendimiento de los sistemas manejados y no se genere latencia en la entrega de la información emitida por la entidad, preferiblemente que el análisis de la información se efectué en la nube.
5. Debe permitir aplicar políticas basadas en el contexto de usuario, tipo de dispositivo y/o aplicación, instancia SaaS (ej.: Salesforce o coreo personal) e IaaS (eje: gestor documental OnBase, NAS), contenido del documento, entre otros, debe ser capaz de inspeccionar en profundidad y entender las diferentes actividades o políticas configuradas (bloquear, autorizar, entre otros.)
6. Debe permitir detectar, analizar, bloquear si el dato es sensible, alertar y con base a la actividad realizada por el usuario solicitar la justificación de su acción que está realizando a fin de proceder o negar la actividad, permitiendo educar al usuario sobre el riesgo del uso de aplicaciones. (est~~a~~e ítem ~~opción~~ puede ser opcional)

7. La solución debe incluir un módulo de protección contra amenazas, con el fin de evitar que los archivos validados contengan virus o alguna amenaza en particular
8. La solución debe ofrecer protección y/o integrarse con Office365 para el control del tráfico que cursa sobre el tenant sin importar el dispositivo desde donde se efectúa el acceso (el control se debe realizar sobre la suit de office365, SharePoint, Teams entre otros que maneje la herramienta).
9. La solución debe garantizar que el agente del DLP debe actuar en todo momento de conexión aplicando las políticas del servidor DLP descritas en la nube, con eso cubriría equipos locales dentro de las instalaciones, equipos portátiles fuera de las instalaciones en modo teletrabajo y equipos celulares o móviles que estén también fuera de la red controlando el tráfico de información aun cuando el dispositivo no cuente con un dominio.
10. La solución debe contar con el cumplimiento para la ley 1581 del 2012 de protección de datos personales del gobierno colombiano o las que la modifiquen.
11. La gestión y remediación de incidentes relacionados con DLP podrá ser flexible en la manera del manejo del reporte de actividades, la misma podrá manejarse dentro de la herramienta y/o contar con un software adicional con el fin de realizar el seguimiento de los mismos.
12. La solución DLP debe tener la habilidad para cubrir todos los métodos de acceso (navegadores, apps móviles, apps de escritorio, entre otros).
13. La solución de Email DLP no debe almacenar correos electrónicos, sólo debe analizar, monitorear y calificar la información en ellos (basados en perfiles DLP) y de esta manera permitir que el servidor de correo electrónico accione.
14. Todos los perfiles de DLP creados deben integrarse o cruzarse sin ninguna configuración adicional en las reglas que se creen de Email DLP o de servicios web.
15. La solución debe estar en la capacidad de generar alertas, validar comportamientos y notificar a terceros en caso de incidencias y/o mal uso de los servicios.
16. La solución debe disponer de una base de datos de Servicios SaaS, en la que se pueda ver el nivel de riesgo de los servicios consumidos y se debe actualizar de forma continua.
17. La solución debe permitir implementar políticas para generar una alerta al usuario donde se indique los riesgos a tener en cuenta y con base a la actividad realizada por el usuario solicitar la justificación de su acción a fin de proceder o negar la actividad, permitiendo educar a los usuarios cuando consumen cierto tipo de aplicaciones. (Este item puede ser opcional)
18. La solución debe tener capacidad de diferenciar entre instancias de aplicaciones tales como gestionadas-corporativas vs instancias de terceros corporativas vs instancias personales y usar la diferenciación a la hora de aplicar reglas de DLP
19. La solución debe conectar a los usuarios remotos directamente a las aplicaciones en entornos de nube pública sin la necesidad de pasar por la infraestructura corporativa
20. La solución debe permitir identificar una instancia personal en una aplicación corporativa para así ejercer un control granular sobre ella.
21. La solución debe permitir la ingesta y exportación de Indicadores de Compromiso (IOCs) de forma automática y ser aplicados únicamente en las instancias de las aplicaciones donde se quiere bloquear o permitir. Este ítem se puede presentar de manera opcional.
22. La solución debe tener la capacidad de entender el comportamiento de los usuarios, distinguiendo la actividad normal anómala, creando índices de comportamiento (IoBs).
23. La solución debe tener capacidad de integración y operaciones sobre distintas plataformas de SO.
24. La solución debe permitir efectuar excepciones en el tráfico en la descripción SSL

25. La solución debe permitir personalizar las notificaciones con logos de la organización.
26. La solución debe permitir personalizar los mensajes que se envían a los usuarios, pudiendo generar mensajes específicos para incumplimiento de políticas.
27. La solución propuesta debe contar con soporte por parte del fabricante teniendo en cuenta los ANS establecidos.
28. La disponibilidad del servicio debe estar garantizada por un acuerdo de nivel de servicio (SLA) de 99,95% para los servicios en línea.
29. La solución debe soportar 1500 usuarios simultáneos (esta deberá contemplar usuarios móviles y servidores si es el caso)
30. La aplicación debe mantener recursos del servicio (performance de la herramienta) por debajo del 75%.
31. La solución debe permitir el acceso a la a la consola central para validaciones, reportes y/o estadísticas de la misma al equipo de seguridad informática de LA PREVISORA S.A.
32. El servicio entregado debe contar con personal externo si así lo considere para soportar la operación en caso de que el soporte dedicado no se encuentre disponible por un caso esporádico.

2. Se modifica el numeral **3. De orden técnico (Capacidad técnica) ítem 21. Certificaciones del proveedor de los ASPECTOS HABILITANTES del capítulo III del documento de condiciones,** el cual quedará de la siguiente manera expresado en color rojo:

21. Certificaciones del proveedor

EL PROPONENTE o Fabricante de la solución deberán allegar con su propuesta las siguientes certificaciones: Certificación ISO 27001. Esta norma permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

La certificación solicitada debe estar vigente a la fecha de presentación de oferta, la firma del contrato y mantenerla vigente durante la vigencia del contrato

3. Se modifica el numeral **3. De orden técnico (Capacidad técnica) ítem 21. Certificaciones del proveedor de los ASPECTOS HABILITANTES del capítulo III del documento de condiciones,** el cual quedará de la siguiente manera expresado en color rojo:

a. Experiencia técnica habilitante

Con el fin de cumplir con la experiencia mínima habilitante, **EL PROPONENTE** deberá adjuntar con su propuesta máximo tres (3) certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma:

- El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista soluciones y/o plataformas relacionadas con Protección de informacion, CASB, Security Service Edge y DLP (fuga de Información).
- El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al 50% del valor del presupuesto.
- El plazo de ejecución de cada contrato certificado incluidas sus prórrogas deberá ser igual o mayor a 12 meses.
- Los contratos certificados deben haberse ejecutado en su totalidad y/o estar en ejecución como mínimo (6) seis meses en operación.

(…)

4. Se modifica el numeral **3. De orden técnico (Capacidad técnica) ítem a. Recurso Humano de los ASPECTOS HABILITANTES del capítulo III del documento de condiciones,** el cual quedará de la siguiente manera expresado en color rojo:

a. Recurso humano

(…)

UN (1) GERENTE DE SERVICIO: Un (1) Gerente de Servicio que estará durante el tiempo total del contrato (Implementación y operación). Mínimo con una dedicación del 20% semanal, pero deberá contar con disponibilidad del 100% del tiempo, cuando sea requerido por **LA PREVISORA S.A.** EL PROPONENTE debe garantizar la disponibilidad del Gerente de Servicio, en forma presencial y/o remota cada vez que **LA PREVISORA S.A.** lo requiera durante el tiempo de ejecución del contrato. El Gerente de Servicio es la persona encargada de la parte operativa y único canal entre las partes, de manera administrativa durante la vigencia del contrato. (condición acreditada con hoja de vida acompañada de los diplomas o actas de grado correspondientes.) Este recurso deberá tener vinculación laboral y/o prestación de servicios directa con EL PROPONENTE.
Perfil Profesional
Profesional en Ingeniería (Sistemas, Electrónico, telecomunicaciones o carreras afines), con especialización y/o maestría en Seguridad Informática y/o doctorado en áreas afines de seguridad informática, Seguridad de la información, seguridad en las TIC o Gerencia de Proyectos de tecnología. Contar con al menos una (1) de las siguientes certificaciones de seguridad o sus equivalentes:

(CSIH) Certified Computer Security Incident Handler - ISACA (CISA) Certified Information Systems Auditor - ISACA (CISM) Certified Information Security Manager - ISACA (CRISC) Certified in Risk and Information System Control – ISACA (CISSP) Certified Information Systems Security Professional - (ISC)² (CSA) Cyber Security Audit - ISACA ISO/IEC 27032 Lead Cybersecurity Manager ISO 27001:2013 o superior Certificación Internacional Auditor Líder ISO 31000:2018 Certificación Internacional Risk Manager (GCPM) GIAC Certified Project Manager – SANS (GSLC) GIAC Security Leadership – SANS (PMP) Project Management Certification
Experiencia
Demostrar experiencia profesional de cinco (5) años y específica como Gerente de Servicio, director de proyectos, gerente de proyectos y/o gestor de proyectos~~servicios~~ por tres (3) años durante los últimos cuarenta y ocho (48) meses, mínimo en dos (2) proyectos de Seguridad y/o Ciberseguridad. Esta debe ser demostrada con certificaciones laborales, emitidas por la empresa en la que labora o por las empresas donde desarrollo proyectos.

Cantidad de hojas de vida:	(1) UNA

Actividades Mínimas
El Gerente de Servicio deberá: • Atender directamente todos los requerimientos de **LA PREVISORA S.A.** • Controlar la calidad del proyecto. • Convocar las reuniones de seguimiento necesarias. • Elaborar y firmar las actas de reuniones de seguimiento y entregables de cada etapa. • Velar por que se cumplan los objetivos contractuales, el alcance, el plan de trabajo que se requiere para el logro del objetivo del proyecto • Coordinar la asignación y actividades de todos los recursos asignados al proyecto. • Mantener el proyecto encaminado en sus objetivos y emitir las acciones correctivas, preventivas y de mejora para lograr el alcance del proyecto en el tiempo y costos definidos.

ADMINISTRADOR DEDICADO
EL PROPONENTE deberá disponer de un ingeniero con experiencia en instalación, configuración y administración de la solución a implementar para prevención de fuga de información, en modalidad remota y/o presencial, cuando sea requerido y disponibilidad fuera de horario por demanda sin costo adicional para **LA PREVISORA S.A.**, durante toda la ejecución del contrato.
Perfil Profesional y Experiencia
Profesional en Ingeniería de sistemas, electrónica, telecomunicaciones o afines con mínimo (2) años de experiencia como administrador de soluciones DLP. Tendrá la responsabilidad De la operación (administración, identificación y gestión de la plataforma), así como las respectivas acciones de mejora sobre la misma.
Certificaciones
El personal, deberá adjuntar la certificación de la solución a entregar y acreditar al menos (1) de las siguientes certificaciones o su equivalente en seguridad: ECIH – EC-Council Certified Incident Handler - EC-Council CNFE – Network Forensic Investigator - Mile2 CHFI – Computer Hacking Forensic Investigator - EC-Council CEH - Certified Ethical Hacker - EC-Council CRISC - Certified in Risk and Information Security Control -ISACA CPTE – Certified Pentester Engineer - Mile2 CPTIA – CREST Practitioner Threat Intelligence Analyst – CompTIA ISO/IEC 27032 Lead Cybersecurity Manager ISO 27001:2013 o superior Certificación Internacional Auditor Líder ISO 27001:2013 o superior Certificación Internacional Auditor Interno ISO 31000:2018 Certificación Internacional Risk Manager

Cantidad de hojas de vida:	(1) UNA

- Proponer solicitudes de cambio con su análisis de impacto y acordar en conjunto con **LA PREVISORA S.A.** la implementación de los cambios que surjan en el proyecto.
- Velar por que todo el equipo asignado por la empresa cumpla con la metodología de proyectos definida por **LA PREVISORA S.A.**
- Identificar y realizar seguimiento a los riesgos identificados para el proyecto y proponer planes de acción para mitigar inconvenientes.
- Realizar el seguimiento y gestión de la ejecución del proyecto.
- Garantizar que todos los entregables cumplan con la calidad y criterios de aceptación definidos con **LA PREVISORA S.A.**

Plantear alternativas de mejoramiento continuo de acuerdo con su experiencia y mejores prácticas.

Actividades Mínimas

- Administrar, gestionar y supervisar la plataforma de prevención de fuga de informacion.
- Garantizar el adecuado uso de la solución y respuesta oportuna a incidentes
- Generar los reportes y el seguimiento de la solución
- Presentar opciones de mejora y afinamiento de la solución.
- Atender los casos relacionados con la plataforma y efectuar el seguimiento respectivo.
- Mantener al día la plataforma y la documentación de la misma.
- Apoyar al interno en los proyectos donde intervenga la prevención de fuga de información.
- Realizar y entregar informes precisos y oportunos sobre el proyecto a la Subgerencia de Infraestructura y Servicios de TI de **LA PREVISORA S.A.**
- Realizar el seguimiento y gestión de la ejecución del proyecto.
- Garantizar que todos los entregables cumplan con la calidad y criterios de aceptación definidos con **LA PREVISORA S.A.**
- Apoyar en los requerimientos, reuniones y entregas de documentación a los diferentes entes de control.

Para que una certificación de experiencia se considere válida, deberá cumplir las siguientes condiciones:

- Nombre y NIT de la empresa contratante
- Fecha de inicio del contrato
- Fecha de terminación del contrato.
- Cargo y funciones desarrolladas. En caso de que las funciones no hayan sido desarrolladas directamente para la empresa que expide la certificación (por ejemplo, una certificación de una empresa mediante la cual el profesional prestó sus servicios a una compañía cliente), debe incluirse la relación de los contratos en los que se participó, incluyendo la compañía, cliente, objeto del contrato, dedicación porcentual y fechas de inicio y fin de la participación* De todas formas, dentro de la certificación aportada o los documentos adicionales que se presenten, se debe contar con el detalle de las funciones, las cuales deben estar directamente relacionadas con los servicios objeto a contratar y el cargo de la persona.
- Deberá estar firmada por el representante legal, gerente o director de recursos humanos o quien haga sus veces o funcionario competente, supervisor del contrato.

(...)

Esta adenda podrá ser consultada en la página web: https://www.previsora.gov.co.

Dada en Bogotá, el 7 de marzo de 2023,

GUSTAVO ADOLFO RAAD
Vicepresidente de Desarrollo Corporativo

Proyectó: Leydi Padilla – Técnico de Contratación
Lorena Pedroza – Especialista Subgerencia de Infraestructura y servicios de TI
Revisó: Jimmy Albornoz - Supervisor del Contrato
Mayerly Lopez – Gerente de Tecnología de la Información
Juan Diego Orozco – Subgerente de Infraestructura y servicios de TI
Scarlett Jordana Baena-Gerente de Contratación (E)