4.4

Bogotá D.C.,

Asunto: SOLICITUD DE INFORMACIÓN PARA ESTUDIO DE MERCADO

Respetados señores:

Atentamente solicito su colaboración, a efectos de obtener información para consolidar estudios de mercado sobre los bienes, obras y/o servicios que se citan a continuación:

<table>
<tr><td>OBJETO</td><td colspan="3">Adquirir la renovación de la suscripción de la herramienta de Gestión del Acceso con Privilegio (PAM – Beyond Trust) y la adquisición del módulo de Detección y Respuesta ante Amenazas de Identidades.</td></tr>
<tr><td rowspan="4">UNSPSC</td><td>CÓDIGO UNSPSC</td><td colspan="2">DESCRIPCIÓN</td></tr>
<tr><td>43212200</td><td colspan="2">Sistemas de manejo de almacenamiento de datos de computador</td></tr>
<tr><td>81111900</td><td colspan="2">Sistemas de recuperación de información</td></tr>
<tr><td>81111800</td><td colspan="2">Servicios de sistemas y administración de componentes de sistemas</td></tr>
<tr><td rowspan="2">DESCRIPCIÓN Y/O ALCANCE</td><td colspan="2">ESPECIFICACIONES TÉCNICAS MÍNIMAS</td><td>COTIZACIÓN ALTERNATIVA</td></tr>
<tr><td colspan="2">Ver ANEXO No. 1 - REQUERIMIENTOS TÉCNICOS MÍNIMOS</td><td>En caso de que aplique o se requieran</td></tr>
</table>

PLAZO PARA EJECUCIÓN-	El plazo para la ejecución del contrato que se suscriba será hasta el 15 de diciembre de 2025, contado a partir de la fecha de aprobación de las garantías, previa expedición del registro presupuestal **Vigencia del soporte y actualización de la herramienta:** Tendrá una duración de 1 año contado a partir del 1 de diciembre del 2025, previo cumplimiento de requisitos de ejecución.
PLAZO PARA LA ENTREGA DE LOS BIENES Y/O SERVICIOS	Se deberá entregar el documento que acredite la entrega y activación a nombre del Ministerio de Hacienda y Crédito Público de 70 licencias de la herramienta de Gestión del Acceso con Privilegio (PAM) Beyond Trust, así como la entrega y puesta en marcha del Módulo de Detección y Respuesta ante Amenazas de Identidades para 1300 usuarios o identidades, incluido el soporte y actualización. El plazo máximo para la entrega del documento será el 9 de diciembre de 2025, fecha en la cual deberá iniciar la renovación del soporte y actualización de la herramienta en mención.
LUGAR DE EJECUCIÓN	Para todos los efectos, el lugar de ejecución del contrato será en la ciudad de Bogotá, D.C. en las instalaciones del Ministerio de Hacienda y Crédito Público: Edificio San Agustín (Cra. 8 No. 6C-38), en la sede Casas de Santa Bárbara (carrera 6 No 6B-55) de manera presencial en sitio y/o de manera virtual en el evento de requerirse, previa autorización del Supervisor del contrato, bajo herramientas tecnológicas autorizadas por el Ministerio de Hacienda y Crédito Público.
FORMA DE PAGO	EL MINISTERIO pagará al CONTRATISTA, **una vez se encuentre aprobado el P.A.C. (Programa anual mensualizado de caja)**, el valor del contrato en **un solo pago en el año 2025**, previa entrega del documento que acredite la suscripción del

	licenciamiento solicitado y firma del acta de recibo a satisfacción por parte del contratista y el supervisor del contrato. Dicho pago se efectuará **con sujeción a la disponibilidad del PAC**, dentro de los diez (10) días hábiles siguientes a la radicación en la Subdirección Financiera y la debida presentación de la factura y del cumplido expedido por el supervisor designado, la certificación de pago de aportes parafiscales y de seguridad social por parte del contratista y registro de carga de dichos soportes en SECOP II.
VALIDEZ DE LA COTIZACIÓN	El Ministerio de Hacienda y Crédito Público requiere que la cotización tenga validez **como mínimo** de Noventa (90) días Calendario. En la cotización debe relacionar su período de validez

COTIZACIÓN ALTERNATIVA *	
Detallar: CUANDO COMPRENDA VARIOS ÍTEMS, SE DEBE COTIZAR INDIVIDUALMENTE CADA UNO	**VALOR UNITARIO**
VALOR TOTAL (incluido IVA)	

NOTA: Si el cotizante encuentra que algo falta, no es procedente o es diferente a lo consignado en la descripción técnica de la necesidad, es importante que lo manifieste, justificando la razón que sustenta el cambio, para que el Ministerio, previo análisis, determine la procedencia de la sugerencia. Para tal fin deberá determinar los costos de la cotización alternativa.

Agradecemos se sirva remitir la información respectiva a más tardar el día **27 de agosto de 2025**, a través de los correos electrónicos invtecnologia@minhacienda.gov.co o laura.chamorro@minhacienda.gov.co

La presente solicitud de información a cotizar fue elaborada por la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público.

Firmado digitalmente por Luis Orlando Arenas Ruiz

LUIS ORLANDO ARENAS RUIZ
Asesor 1020 - 8 – Subdirección de Ingeniería de Software

HUERTAS ORTIZ DIEGO FERNANDO
Firmado digitalmente por HUERTAS ORTIZ DIEGO FERNANDO
Fecha: 2025.08.20 15:56:28 -05'00'

Vo.Bo. DIEGO FERNANDO HUERTAS ORTIZ
Director de Tecnología

Anexos:
ANEXO No. 1 - REQUERIMIENTOS TECNICOS Y OBLIGACIONES MÍNIMAS.
ANEXO No. 2 – COTIZACIÓN ECONOMICA
ANEXO No. 3 - INFORMACIÓN ADICIONAL

* Si el cotizante desea presentar una cotización alternativa a la solicitada por el Ministerio, debe cumplir con las condiciones técnicas mínimas de la cotización básica.

Revisado DT: Laura Chamorro / Laura Duran

ANEXO No. 1

REQUERIMIENTOS TÉCNICOS Y OBLIGACIONES MÍNIMAS

Entrega y activación a nombre del Ministerio de Hacienda y Crédito Público de 70 licencias de la herramienta de Gestión del Acceso con Privilegio (PAM), Beyond Trust y la adquisición del módulo Detección y Respuesta ante Amenazas de Identidad para 1300 licencias, con las siguientes características mínimas:	
CARACTERÍSTICAS GENERALES DE LAS HERRAMIENTAS	
1.1	**Administración centralizada de Credenciales y Manejo de activos y descubrimientos**
1.1.1.	La herramienta debe estar disponible como entorno físico o virtual con infraestructura (servidores / software entorno virtual, Sistema Operativo)
1.1.2.	Permitir el Descubrimiento de activos, procesos, servicios y credenciales para ser aprovisionadas en el sistema.
1.1.3.	Permitir el manejo de repositorios de cuentas AD / AzureAD / Web / Bases de Datos / Cloud / Dispositivos de red / Aplicaciones /mainframes, así como el manejo de cuentas que no son administradas de forma centralizadas por los servidores de directorio activo.
1.1.4.	Crear credenciales y llaves con diferentes niveles de complejidad
1.1.5.	Realizar el cambio de contraseñas de servicios al reiniciar servicios de Windows. Reemplazar las contraseñas con privilegios que están siendo utilizadas por un servicio determinado en las ubicaciones donde se utilizan. Realizar de manera secuencial o en cascada a medida que se hace la detección; automática mediante búsquedas en directorios activos (AD) y segmentos de dirección IP.
1.1.6.	Contar con la capacidad para poder realizar cambios y rotación de credenciales en archivos o códigos donde se encuentren credenciales privilegiadas.
1.1.7.	Contar con la capacidad para gestionar llaves SSH y descubrimiento de las mismas.

1.1.8.	Permitir la Integración con sistemas de aplicaciones para poder brindar credenciales vía API y evitar la configuración de credenciales estáticas en los sistemas mediante código como Python, C #, Java, PowerShell, Ruby y Unix Shell Script.
1.1.9.	Segregar el acceso a credenciales basado en roles y responsables (RBAC) Control de acceso basado en roles (es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al superusuario) para tener una granularidad el acceso.
1.1.10.	Permitir la definición de flujos de aprobación para obtener accesos a las cuentas privilegiadas, con características tales como: personalización de flujos para su aprobación, determinar la criticidad, características de cuentas, definir los responsables, aprobación para acciones administrativas.
1.1.11	Permitir la autenticación dinámica basadas en contexto de riesgo de seguridad, a través de la creación de un perfil o perfiles, para los usuarios, aprovechando los atributos situacionales del mismo, tales como ubicación, el dispositivo, la red, el horario, solicitud previa de aprobación o auto aprobaciones, restricciones para ejecutar acciones incluso solo mirar la actividad de un tercero.
1.1.12.	Contar con la capacidad de carga masiva para importar sistemas administrados, cuentas privilegiadas, usuarios y otros objetos necesarios.
1.1.13.	Contar con la capacidad de registrar la información de los sistemas administrados como: la dirección IP, la dirección MAC, el nombre DNS, el propietario del sistema, el tipo de plataforma y la versión, listado de cuentas y sus estados en sistemas operativos.
1.1.14.	Permitir al administrador definir atributos personalizados tanto para el sistema administrado, como para las cuentas privilegiadas.

1.1.15.	Contar con la capacidad de descubrir, inventariar y cambiar credenciales de todas las cuentas privilegiadas para los siguientes sistemas: Windows • Linux • Hipervisores • Mac OS • Directorios (AD / LDAP) • Bases de datos • Dispositivos de red (LAN/WAN) • Equipos de Seguridad Informáticos y Seguridad • Aplicaciones /ej. SalesForce, Instagram, Sql estudio o aplicaciones desarrolladas Inhouse)
1.1.16.	Contar con la capacidad para detectar servicios de Windows, tareas programadas y administrar automáticamente las credenciales privilegiadas.
1.1.17.	Contar con la capacidad de descubrir nuevas cuentas privilegiadas y de incorporarlas automáticamente para la gestión de contraseñas.
1.2.	**Gestión de Sesiones Remotas**
1.2.1.	Contar con la capacidad de entregar accesos remotos seguros a los usuarios corporativos o externos, sin necesidad de instalación de clientes VPN en los dispositivos de usuarios remotos y garantizando un acceso seguro con MFA sin necesidad de modificar los recursos de autenticación corporativos como el AD, estos servicios se deben prestar durante todo el periodo de suscripción de renovación.
1.2.2.	Proveer un portal de acceso y no requerir la instalación de agentes o clientes en los dispositivos de origen.
1.2.3.	Permitir que el administrador utilice listas blancas y listas negras para evitar movimientos laterales.
1.2.4.	Permitir la restricción de comandos específicos o scripts.
1.2.5.	Evitar que aplicaciones de terceros no autorizadas puedan ser ejecutadas desde una sesión remota.
1.2.6.	Controlar él envió o descarga de archivos, así como el copiado al portapapeles.
1.2.7.	Realizar restricciones de acceso por horarios.

1.2.8.	Realizar la invitación de nuevos usuarios para tener una sesión compartida con la opción de chat para comunicación.
1.2.9.	Permitir el establecimiento de conexiones vía RDP, SSH (SUDO), Túneles TCP, WEB sin uso de licenciamiento adicional como Microsoft RDS.
1.2.10.	Realizar grabación e indexación de cada sesión privilegiada mediante video aprueba de manipulación, permitiendo que los comandos en los videos generados se puedan indexar para futuras búsquedas, permitiendo el filtro de comandos y acciones realizadas a lo largo de la sesión, lo que le permite buscar acciones específicas en la sesión grabada.
1.2.11.	Contar con la capacidad de configurar scripts para ser ejecutados en los dispositivos remotos (Linux/Unix/Windows/powershell).
1.2.12.	Permitir el registro de auditoría de la sesión y las actividades que realiza el usuario como aplicaciones que ejecuta.
1.2.13.	Permitir el acceso a líneas de comando o llaves de registro en sistemas Windows sin compartir la pantalla para un consumo bajo de ancho de banda.
1.2.14.	Permitir la Inyección de credenciales para evitar la manipulación de password privilegiados para usuarios o terceros.
1.2.15.	Impedir la elevación de privilegios y ejecución de aplicaciones con privilegios elevados cuando se utiliza un agente de conexión
1.2.16.	Contar con la capacidad de ejecutar múltiples sesiones de forma simultánea, como soportar múltiples monitores (remote desktop).
1.2.17.	Contar con la capacidad de invitar a usuarios internos o externos para compartir una sesión remota con o sin privilegios sin impactar el equipo accesado.
1.2.18.	Contar con la capacidad de realizar el acceso con agente (sin protocolos estándares) o sin agente (con protocolos estándares) dependiendo del modelo de conectividad.
1.3.	**Auditoria, reportería y analítica**
1.3.1.	Permitir identificar el comportamiento de los usuarios, reflejando las tareas y comportamientos inusuales
1.3.2.	Respaldar la auditoría y la rendición de cuentas donde se registra cada transacción para cada solicitud.

1.3.3.	Contar con la capacidad de capturar todos los cambios realizados por los administradores en la pista de auditoría, incluido el nombre de usuario, la marca de tiempo, la actividad realizada, la dirección IP y los valores antiguos / nuevos.
1.3.4.	Contar con la capacidad de generar todos los informes por frecuencia, bajo demanda o como tareas programadas, así mismo deberá admitir mínimamente estos formatos de informe: CSV, Excel, PDF, PowerPoint, MHTML, Word, TIFF y XML, y admitir contenido de informes enriquecido que incluye, entre otros, texto, tabla, gráficos, gráfico, barra, etc.
1.3.5.	Permitir el descubrimiento, gestión de passwords, credenciales y sesiones
1.3.6.	Proporcionar los siguientes tipos de informes listos para usar sin ningún componente adicional y sin costo adicional: • Informe de antigüedad de contraseña de cuenta que proporciona la última fecha y fecha de cambio de contraseña para cada cuenta administrada. • Informe de actividades del usuario que proporciona una vista transaccional detallada de las actividades de aprobación y solicitud de sesión y contraseña. • Informe de derechos que detalla quién tiene acceso a qué cuentas. • Informe de actividad de cambio de contraseña que detalla el motivo y el resultado del cambio de contraseña. • Informe de programación de cambio de contraseña que proporciona detalles del próximo cambio de contraseña programado. • Restablecimiento de contraseña al liberar el informe de conciliación que muestra los estados de restablecimiento de finalización de solicitud de contraseñas de cuentas administradas para proporcionar evidencia auditable de que las contraseñas se han restablecido adecuadamente después de ser liberadas. • Informe de inventario de activos que proporciona una lista de todos los sistemas administrados y no administrados, activos de TI descubiertos agrupados por sistema operativo. • Informe de inventario de cuenta que proporciona una lista de todas las cuentas administradas y no administradas.

	• Informe delta de cuenta que proporciona cambios delta para cuentas agregadas y eliminadas de acuerdo con períodos diarios, semanales y mensuales.
	• Informe de cuentas administradas vs no administradas que proporciona una lista de cuentas del sistema de destino e indica cuáles están bajo administración de contraseñas.
	• Informe de uso de la cuenta de servicio que proporciona una lista detallada de qué sistemas están utilizando una cuenta de servicio para iniciar uno o más servicios de Windows.
	• Informes que proporcionen visibilidad a la operación tales:
	  ○ Top usuario usados por plataforma
	  ○ Top de dispositivos a los que se conectan
	  ○ Salud del sistema, alertas y fallas
	  ○ Cuentas que no han rotado en el sistema
	  ○ Top duración de las sesiones
	  ○ Top de las sesiones más altas
	  ○ Actividad semana
	  ○ Navegadores más usados para el acceso de portal web
	  ○ Utilización de motor de análisis de comportamiento de los usuarios

1.3.7.	Contar con la capacidad de permitir la creación de informes personalizados.
1.3.8.	Contar con la capacidad de exportar sesiones y grabaciones para extender el almacenamiento y análisis posteriores.
1.3.9.	Permitir la Integración con múltiples sistemas SIEM para la extensión de la correlación y análisis de anomalías /riesgos.
2.	**Módulo Detección y Respuesta ante Amenazas de Identidad**
2.1.	La solución debe contar con una consola web optimizada para HTML5, compatible con al menos los siguientes navegadores: • Microsoft Edge • FireFox • Google Chrome • Safari

2.2.	La solución debe descubrir identidades, cuentas y privilegios en todo el entorno de identidad del Ministerio, tanto local como en la nube y SaaS.
2.3	Debe proporcionar una visión holística de las identidades y el acceso a toda la infraestructura de TI
2.4	Debe ser capaz de identificar cuentas privilegiadas con permisos excesivos, controles de seguridad deficientes y anomalías.
2.5	La solución debe proporcionar recomendaciones prácticas antes de que se conviertan en una amenaza y agilizar la investigación de amenazas potenciales.
2.6	La herramienta debe evaluar, ajustar y prevenir permisos excesivos de identidades de personas y máquinas.
2.7	La solución debe aprovechar los recursos y la inteligencia de los productos de gestión de privilegios y otras soluciones conectadas.
2.8	Debe ser posible organizar varias organizaciones en una misma consola, permitiendo así seleccionar de forma centralizada a qué unidad organizativa pertenecen los eventos de identidad.
2.9	Debe proporcionar un monitoreo continuo de las actividades de los usuarios y entidades en búsqueda de comportamientos anormales y sospechosos.
2.10	Debe realizar la detección de acceso no autorizado, escalada de privilegios y movimiento lateral.
2.11	Debe identificar amenazas como phishing, malware e ingeniería social.
2.12	Debe ser posible crear perfiles de comportamiento de usuarios y entidades basados en actividades históricas.
2.13	Debe tener detección de anomalías y desviaciones del comportamiento normal.
2.14	Debe tener funcionalidad para analizar actividades en diferentes contextos, como tiempo de acceso, ubicación y dispositivos utilizados.
2.15	Debe ser posible realizar una investigación en profundidad de los incidentes de seguridad relacionados con la identidad.
2.16	Debe correlacionar eventos de diferentes fuentes para identificar la causa raíz del comportamiento o acción sospechosa.

2.17	Debe proporcionar herramientas para contener las amenazas o amenazas encontradas, como el bloqueo de cuentas, el restablecimiento de contraseñas y la revocación de acceso.
2.18	El panel de control de la solución debe tener no exclusivamente, sino al menos las siguientes vistas: • Representación de integraciones con fuentes de datos de terceros • Número total de identidades descubiertas por la solución • Vista de cuentas privilegiadas descubiertas, cuentas con perfil administrativo o cuentas de usuario que son miembros de grupos de seguridad • Lista de cuentas inactivas o cuentas que no han sido utilizadas durante un período de tiempo determinado o que no han cambiado su contraseña en el último año • Resumen de identidades potencialmente comprometidas • Resumen de elementos que tienen permisos elevados, como cuentas o identidades, permitiendo monitorear el acceso. • Proporcionar una vista de las recomendaciones de seguridad, lo que permite al administrador verificar el estado y la corrección necesaria de las detecciones automáticas.
2.18	La solución debe permitir la creación de perfiles de usuario y cada usuario debe tener reglas específicas para el acceso a las unidades organizativas.
2.19	Debe ser posible automatizar tareas repetitivas de análisis e investigación de incidentes.
2.20	Debe ser posible implementar medidas de respuesta automatizadas para contener amenazas. • Debe ser posible la integración con otras herramientas a través de la integración API para estas funcionalidades.

2.21	Debe permitir una visión unificada de las identidades y los riesgos relacionados en todo el ecosistema de identidades. Esta visión debe incluir al menos los siguientes sistemas: • Microsoft Active Directory • Microsoft Entra ID • Okta • Azure AD • AWS • Google Cloud • GitHUB
2.22	Debería ser posible mitigar los riesgos de identidad, como privilegios mal protegidos, rutas de escalada de privilegios y configuraciones erróneas con recomendaciones prescriptivas.
2.23	Debería ser posible detectar amenazas basadas en la identidad, como el abuso de privilegios y el acceso a la infraestructura.
2.24	Debería permitir a los administradores ver los privilegios de los usuarios.
2.25	Debe aplicar el principio del mínimo privilegio y remediar las amenazas basadas en la identidad.
2.26	La solución debe permitir la creación de reglas de exclusión para detecciones, identidades y recomendaciones.
2.27	Debe ser posible crear integraciones a través de WebHook
2.28	Debe ser posible cambiar y monitorear incidentes directamente en la consola de la solución, con las siguientes opciones: • Nuevo • En revisión • Resuelto • Falso Positivo • Ignorado
2.29	Debe ser posible automatizar acciones proactivas a través de integraciones.
3	**HORARIO PARA LA PRESTACIÓN DEL SERVICIO**

	Los servicios de soporte y mantenimiento técnico se prestarán de lunes a viernes, en horario de 8 am a 5 pm. Los plazos en horas se contarán dentro del horario establecido de tal forma que un plazo estipulado de cuatro horas que empiece a contar a las 4:00 p.m. se suspenderá a las 5:00 p.m. para continuar al día siguiente a partir de las 8:00 a.m., terminando el plazo para este caso, a las 11:00 a.m. del día hábil siguiente. Sin embargo, previo acuerdo con el supervisor del contrato, se pueden realizar las actividades que se consideren en un horario diferente al antes señalado.
4	**ACTIVIDADES DE INICIO DEL CONTRATO:** Las siguientes actividades se acordarán con el supervisor del contrato con el fin de programarlas dentro de los diez (10) primeros días hábiles siguientes al inicio del contrato: a. Realizar la entrega y activación de versionamiento por 1 año, de las licencias **b.** Proporcionar acceso en línea a través de Internet a las páginas de referencia del fabricante, a la base de datos de conocimiento y a los foros del fabricante referentes a la herramienta instalada en el Ministerio, permitiendo registrar allí como mínimo a cinco (5) ingenieros de la Dirección de Tecnología del Ministerio. **c.** Realizar una revisión en sitio (o de manera remota si las circunstancias lo requieren) del estado de operatividad de la herramienta, después de registrar el licenciamiento del software, las configuraciones implementadas en la herramienta, de manera que se disponga de un estado de las condiciones de funcionamiento en que se hayan encontrado éstas. **d.** En caso de considerarlo necesario y crítico para el funcionamiento de la herramienta, planear y realizar el cambio de las configuraciones de acuerdo con los resultados obtenidos, en coordinación con el supervisor del contrato o responsable técnico, con el fin de mantener la herramienta en correcto funcionamiento, según las recomendaciones del fabricante y mejores prácticas del mercado.

	Una vez finalizada la visita, entregar al Ministerio un informe que consolide las actividades y resultados de las acciones ejecutadas
5	**ACTUALIZACIÓN DE VERSIONAMIENTO** Actualización del Software: Debe cubrir todas las actualizaciones del software a la última versión liberada por el fabricante, así como parches o "fixes" liberados en el mercado de acuerdo con las recomendaciones del fabricante, para lo cual el contratista debe planear y aplicar dichas actualizaciones a todos los equipos que hacen parte de la herramienta ofertada sin costo adicional para el Ministerio de Hacienda y Crédito Público, durante el tiempo de vigencia del contrato. Adicionalmente se debe prestar un servicio de apoyo, atención y solución a los incidentes y requerimientos que se presenten en la herramienta de identidades y privilegios instalada durante el tiempo de vigencia del contrato. Por incidente se entenderá todas las eventualidades que generen problemas técnicos como fallas, daños, degradación del desempeño, mal funcionamiento o anomalías que se presentan en la herramienta y que impidan que esta cumpla con su óptimo desempeño. Por requerimiento se entenderá el servicio de apoyo en el cambio de las configuraciones o afinamientos sobre la configuración de la plataforma objeto del presente contrato. Este servicio consiste en la mejora y optimización de la herramienta del fabricante, así como también la prevención y detección de posibles fallas que se puedan presentar en dicha herramienta. Las actividades que se realicen sobre la herramienta deben ser coordinadas previamente con el supervisor del contrato y, después de la ejecución de las actividades, debe ser entregada la documentación correspondiente donde estén totalmente detalladas las actividades ejecutadas.

	El contratista debe cumplir los siguientes términos para la prestación del servicio: 1. Disponer de un servicio de atención técnica 5x8x365. Responder a la solicitud dentro de un plazo no mayor de una (2) horas contadas a partir de la hora del registro de la solicitud del servicio. 2. Disponer de una línea telefónica para el reporte de los incidentes, los cuales también se podrán reportar a través de correo electrónico o vía Internet. 3. En el momento del reporte del incidente se debe hacer un registro que incluya mínimo los datos de fecha, hora, descripción y número del incidente. El número de incidente asignado se utilizará para identificar y hacer seguimiento del mismo. 4. Prestar asistencia técnica por parte de los ingenieros de soporte de la plataforma mediante atención en: sitio, acceso remoto, vía telefónica, correo electrónico o cualquier otro medio definido entre las partes 5. Prestar un servicio de atención técnica, a través del cual se recibirán los incidentes reportados por el Ministerio de Hacienda y Crédito Público, en el que se deberá hacer un registro que incluya mínimo los datos de fecha, hora y descripción, el cual se utilizará para identificar y hacer seguimiento al caso reportado. Responder al incidente reportado por el Ministerio dentro de un plazo no mayor de dos (2) horas contadas a partir del reporte del mismo. 6. El especialista de soporte dispondrá de máximo 2 horas de soporte remoto, contadas a partir del registro del incidente para solucionarlo. Si en este periodo de tiempo no se soluciona el problema, el incidente deberá ser atendido en sitio, en las sedes del Ministerio de Hacienda y Crédito Público, para lo cual contará con un plazo no mayor de dos (2) horas para el desplazamiento del especialista de soporte, contadas a partir de la finalización de la atención realizada remotamente. 7. Para incidentes de criticidad e impacto bloqueante, que afecten operaciones del Ministerio, serán atendidos en sitio por especialistas

	con experiencia en soporte de problemas y a la vez se debe generar el caso con el fabricante de la plataforma. El especialista contara con un tiempo de dos (2) horas para el desplazamiento contadas a partir del registro del incidente. 8. Los casos que se escalen al centro de atención del fabricante deben ser ilimitados y se deben poder acceder por parte del Ministerio. 9. Las actividades que se generen con ocasión de la actualización y el apoyo deben ser tramitadas y ejecutadas por parte del contratista ya sea para apertura de casos ante el fabricante, nuevas configuraciones y demás actividades que se requieran para la normal operación de la herramienta.
6	**TRANSFERENCIA DE CONOCIMIENTO:** Durante la ejecución del contrato, se debe brindar una (1) transferencia de conocimiento de las últimas versiones certificadas de acuerdo a los estándares establecidos por el fabricante de la herramienta, para mínimo cinco (5) funcionarios del Ministerio de Hacienda y Crédito Público con una intensidad horaria de mínimo de ocho (8) horas; en la cual se provean conocimientos específicos de los fundamentos, administración, operación y manejo de las tecnologías y configuraciones implementadas en la solución, así como temas relacionados con la configuración, operación, integración y resolución de problemas, su realización será coordinada con el supervisor del contrato. Esta transferencia de conocimiento se debe realizar en las instalaciones del Ministerio de Hacienda y Crédito Público o de manera remota si las circunstancias de salud pública así lo exigen. La planeación, programación y realización de esta actividad debe coordinarse con el supervisor del contrato.
7	**GARANTIA Y SOPORTE:** El servicio de soporte técnico se encuentra incluido dentro de la herramienta adquirida y consiste en mantener en perfecto estado de funcionamiento todos los componentes de la plataforma a renovar, por el

	tiempo de vigencia de la suscripción para lo cual el contratista con objeto de dar cumplimiento al contrato que se genere de este proceso deberá a. Prestar este servicio a partir del 01 de diciembre de 2025 hasta el 30 de noviembre del 2026. b. La aplicación de la garantía no puede generar costos adicionales a los especificados en la PROPUESTA. Para tal efecto, el PROPONENTE debe considerar todos los costos de instalación, configuración y los que juzgue necesarios para cumplir efectivamente con el tiempo de garantía ofrecido en la propuesta. Realizar mantenimientos preventivos a la plataforma que hacen parte de la solución, durante la ejecución del contrato. En los casos de actualizaciones críticas la visita deberá realizarse de forma inmediata.
8	**CONFIDENCIALIDAD:** Toda la información correspondiente a diseños, implementaciones, configuraciones, levantamiento de información y los resultados de los mantenimientos y atención de incidentes que realicen los especialistas, así como la información que sea entregada por el Ministerio de Hacienda y Crédito Público dentro de las actividades objeto del contrato serán tratados por el Contratista en forma confidencial, adhiriéndose a las políticas de seguridad y de terceros del Ministerio de Hacienda y Crédito Público.

ANEXO No. 2
COTIZACIÓN ECONÓMICA

Ítem	Descripción	Unidad de medida	Cantidad	Valor Unitario	IVA (si aplica, indicar a que ítem aplica y discriminarlo aquí)	Valor Total
1.	Renovación herramienta gestión del Acceso con Privilegio (PAM) (70 usuarios)	Usuarios	70			
2.	Adquisición Módulo de Detección y Respuesta ante Amenazas de Identidades.	Identidades	1300			
3.	Instalación, despliegue soporte y actualización de versionamiento durante la vigencia del contrato.	Año	1			
4.	Transferencia de conocimiento	Servicio	1			
					TOTAL COTIZACION:	

Los valores se deben registrar en pesos colombianos
NOTA 1: Por favor diligenciar el detalle de cada uno de los ítems
NOTA 2: Los valores se deben ajustar al peso
NOTA 3: Por favor registrar que ítem tiene el pago de IVA o si se encuentra exento del mismo

ANEXO No. 3
INFORMACIÓN ADICIONAL

El cotizante, corresponde a alguna de las siguientes categorías:

	SI	NO
MICRO EMPRESA		
PEQUEÑA EMPRESA		
MEDIANA EMPRESA		

Relacione contratos celebrados relacionados con el objeto cotizado, en los cinco (5) últimos años con otras Entidades Estatales y/o Privadas (número y fecha del contrato, nombre entidad contratante).

No. del Contrato	Fecha del Contrato	Objeto del Contrato	Nombre Entidad Contratante

INFORMACIÓN RELACIONADA CON EMPRENDIMIENTOS Y EMPRESAS DE MUJERES

Por favor diligenciar sí el cotizante se encuentra en alguna de las siguientes definiciones:

DEFINICIONES	SI
Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica pertenezcan a mujeres y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección	
Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel. Entendiéndose como empleos del nivel directivo aquellos cuyas funciones están relacionadas con la dirección de áreas misionales de la empresa y la toma de decisiones a nivel estratégico. En este sentido, serán cargos de nivel directivo los que dentro de la organización de la empresa se encuentran ubicados en un nivel de mando o los que por su jerarquía desempeñan cargos encaminados al cumplimiento de funciones orientadas a representar al empleador.	
Cuando la persona natural sea una mujer y haya ejercido actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior a la fecha de cierre del proceso de selección.	
Asociaciones y cooperativas, cuando más del cincuenta por ciento (50%) de los asociados sean mujeres y la participación haya correspondido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.	

INFORMACIÓN PARA EL FOMENTO DE SUJETOS EN ESPECIAL PROTECCIÓN CONSTITUCIONAL.

El cotizante cuenta con alguno de los siguientes grupos poblacionales, para la provisión de bienes o servicios para la ejecución del objeto cotizado:

GRUPOS POBLACIONALES	SI

Población en pobreza extrema	
Desplazados por la Violencia	
personas en proceso de reintegración o reincorporación	
Víctima del conflicto armado interno	
Mujeres cabeza de familia	
Adultos mayores	
Personas en condición de discapacidad	
Comunidades Indígenas, negra, afrocolombiana, raizal, palanquera, Rom o gitanas	
Otros sujetos de especial protección constitucional	

PROVEEDOR

Nombre o Razón Social del Cotizante _____
Nombre del Representante _____
Nit o Cédula de Ciudadanía No. _____ de_____
Dirección _____
Ciudad _____
Teléfono _____
Fax _____
Correo electrónico _____