CONVOCATORIA PARA LA ELABORACIÓN DEL ESTUDIO DE MERCADO

El Servicio de Rentas Internas (SRI) a través de la Dirección Nacional de Tecnología, convoca a proveedores nacionales e internacionales a participar en el proceso de elaboración del Estudio de Mercado para la "**ADQUISICIÓN DE HERRAMIENTA DE GESTION DE IDENTIDADES**"

Este estudio de mercado será utilizado para la definición del presupuesto referencial previo a la publicación del proceso de adquisición.

El precio referencial de los bienes deberá considerar los siguientes aspectos:

- Las especificaciones técnicas detalladas adelante;
- Los precios cotizados deben estar en valor DDP Delivered Duty Paid/ Entregado con derechos pagados, incluyendo todos los derechos de aduanas e impuestos;
- La vigencia de la cotización no debe ser menor a 120 días;
- La fuente de financiamiento será realizada con recursos del Banco Interamericano de Desarrollo, por lo que los oferentes deberán pertenecer a los países miembros del BID;
- El plazo total de ejecución del contrato será de hasta 1.109 días contados a partir del día siguiente laborable de la suscripción del contrato;

Las cotizaciones deben ser remitidas en formato digital (firmadas) mediante el aplicativo Firma EC, al correo institucional programaintax@sri.gob.ec hasta el 29 de enero de 2024, con los siguientes datos:

Datos del oferente:
Razón Social:
RUC / ID:
Dirección:
Teléfono:
Fecha de emisión de la cotización:
Vigencia de la cotización: (no debe ser menor a 120 días)
Firma de responsabilidad.
CPC: 733100011
Datos del contratante:

A nombre de: Servicio de Rentas Internas
RUC: 1760013210001

Formato Presentación Cotización:

Propuesta Económica:

DESGLOSE DE COMPONENTES				
Tipo de recurso	**Descripción producto / servicio**	**Cantidad**	**Costo unitario**	**Total**
Software	Licencias de software de Gestión de Identidades con soporte de fábrica por 1 año. Incluye activación de Consola de gestión y administración de la herramienta	3142		
Servicios conexos	Soporte extendido de fábrica (2 años adicionales)	2		
Servicios conexos	Implementación y transferencia de conocimientos	1		
Servicios conexos	Soporte Local (3 años)	3		
			Subtotal	$ 0.00
			IVA (12 %)	$ 0.00
			Total	**$ 0.00**

Nota: Los oferentes deberán garantizar el entendimiento y el cumplimiento de todas las especificaciones técnicas y servicios conexos requeridos.

Listado de países elegibles

- Lista de países miembros cuando el financiamiento provenga del Banco Interamericano de Desarrollo: Alemania, Argentina, Austria, Bahamas, Barbados, Bélgica, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Croacia, Dinamarca, Ecuador, El Salvador, Eslovenia, España, Estados Unidos, Finlandia, Francia, Guatemala, Guyana, Haití, Honduras, Israel, Italia, Jamaica, Japón, México, Nicaragua, Noruega, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido, República de Corea, República Dominicana, República Popular de China, Suecia, Suiza, Surinam, Trinidad y Tobago, Uruguay, y Venezuela.

Territorios elegibles

- Guadalupe, Guyana Francesa, Martinica, Reunión – por ser Departamentos de Francia.
- Islas Vírgenes Estadounidenses, Puerto Rico, Guam – por ser Territorios de los Estados Unidos de América.
- Aruba – por ser País Constituyente del Reino de los Países Bajos; y Bonaire, Curazao, Sint Maarten, Sint Eustatius – por ser Departamentos de Reino de los Países Bajos.
- Hong Kong – por ser Región Especial Administrativa de la República Popular de China.

Servicio de Rentas Internas

ESPECIFICACIONES TÉCNICAS

1. INFORMACIÓN QUE DISPONE LA ENTIDAD

A continuación, se detalla el licenciamiento de la Herramienta de Gestión de Identidades implementada actualmente en el SRI:

CANTIDAD	NUMERO DE PARTE	DESCRIPCIÓN
400	D1K0WLL	IBM Security Directory Server Processor Value Unit (PVU) License + SW Subscription & Support 12 Months
400	E0M57LL	IBM Security Directory Server Processor Value Unit (PVU) Annual SW Subscription & Support Renewal
400	E0M57LL	IBM Security Directory Server Processor Value Unit (PVU) Annual SW Subscription & Support Renewal
3500	D61VYLL	IBM Security Identity Manager and Role Management User Value Unit SW Subscription & Support Reinstatement 12 Months
3500	E047RLL	IBM Security Identity Manager and Role Management User Value Unit Annual SW Subscription & Support Renewal
3500	E047RLL	IBM Security Identity Manager and Role Management User Value Unit Annual SW Subscription & Support Renewal

La infraestructura de la Herramienta de Gestión de Identidades implementada actualmente está conformada por los siguientes servidores, sus recursos deberán ser reutilizados para la

implementación de la nueva herramienta, al momento se dispone en total de 34 CPU's, 80 Gb en RAM y 3,2 Tb de almacenamiento:

CANTIDAD	COMPONENTES INSTALADOS	SISTEMA OPERATIVO	FUNCIÓN
2	ISDS	RH 6.4	Servidores donde reside el servicio de LDAP.
2	ISDS Proxy	RH 6.4	Servidores donde reside el servicio de intermediación para las operaciones realizadas contra LDAP.
2	ISIM	RH 6.4	Servidor donde reside la aplicación ISIM.
1	DMGR	RH 6.4	Servidor donde reside el Deployment Manager y el TDI.
2	BD	RH 6.4	Servidores donde reside la base de datos de la solución.

La infraestructura de ambientes virtualizados que dispone el SRI, se encuentra implementada con la plataforma VMWARE ESXi versión 7.0.3.

Al momento se tiene cargados un total de **4.441 perfiles** y **1.865 roles** en la herramienta de Gestión de Identidades implementada actualmente.

2. SERVICIOS REQUERIDOS

2.1. ALCANCE

Licenciamiento y soporte de fábrica

- Licenciamiento de la solución para 3.142 persona por 1095 días.
- Soporte de fábrica para toda la solución por 1095 días.

Implementación y transferencia de conocimientos

- Implementación de la herramienta en los ambientes requeridos y activación del licenciamiento adquirido.
- Personalización de la herramienta con los flujos de automatización solicitados.
- Migración de información de la herramienta actual a la nueva.
- Transferencia de conocimientos impartida de forma presencial. El administrador de contrato entregará el listado de los participantes (9 funcionarios aproximadamente).

Soporte local

- Soporte técnico local sobre incidentes y requerimientos de asistencia sobre la herramienta por 1095 días.
- Visitas técnicas para afinamiento y actualización de la solución por 1095 días.
- El servicio de soporte técnico local debe tener una disponibilidad de 8x5 de lunes a viernes.

2.2. METODOLOGÍA DE TRABAJO

Cláusulas generales

- Todas las actividades que impliquen cambios en la configuración de la Herramienta de Gestión de Identidades deberán ser informados al Administrador del Contrato, y deberán ser aplicados de manera controlada en coordinación con el personal del SRI.
- El personal técnico del contratista deberá contar con todos los medios y recursos necesarios para la ejecución ágil y oportuna de todos los trabajos que son parte del objeto del presente contrato; incluyendo, pero no limitado a: equipo portátil, dispositivos de acceso a Internet (ej. modems), medios removibles de almacenamiento (ej. USB Flash Drives, USB External Hard Drives, etc.), cables de conexión a puertos de consola, "patchcords", y demás artículos o herramientas que se requieran, según cada caso.
- Cualquier acceso que necesite el contratista para cumplir de manera exitosa con los trabajos objeto del presente contrato deberá ser solicitado previamente al Administrador del Contrato con al menos de 5 días calendario de antelación.
- Toda documentación entregada al SRI se dará por recibida únicamente cuando ésta no tenga observaciones y cumpla debidamente con el requerimiento del SRI y aprobación por parte del Administrador del Contrato.
- Todos los gastos incurridos en el cumplimiento del contrato están a cargo del contratista. El SRI no incurrirá en ningún gasto adicional.

Licenciamiento y soporte de fábrica

- El licenciamiento para las 3.142 personas deberá ser activado e incluirá el soporte de fábrica necesario para el normal funcionamiento de la herramienta.
- Durante el periodo de vigencia del soporte de fábrica, el SRI debe tener acceso a:
    - Nuevas versiones de la herramienta y actualizaciones.
    - Acceso para abrir casos directamente con el fabricante.
    - Acceso a la base de conocimientos del fabricante.

Implementación y transferencia de conocimientos

Implementación:

- El contratista deberá entregar al Administrador del Contrato el Plan de Implementación

que incluirá al menos:

- Arquitectura de la solución a ser implementada, incluyendo la versión de software.
- Cronograma de trabajo.

- El contratista deberá desplegar en la infraestructura virtual del SRI la totalidad de la Herramienta de Gestión de Identidades.
- La implementación del licenciamiento de software de Gestión de Identidades deberá ser realizado en su totalidad por el contratista en los ambientes de desarrollo, pruebas, contingencia y producción que incluya la personalización de los flujos automatizados, migración de la información de la herramienta actual a la nueva.

Transferencia de Conocimientos:

- El proveedor debe proporcionar transferencia de conocimientos para el personal del SRI, permitiendo comprender y aprovechar al máximo las funcionalidades de la Solución de Gestión de Identidades.
- La transferencia de conocimientos debe ser impartida de manera presencial en un espacio adecuado para al menos 9 personas con una duración de al menos 20 horas.
- La transferencia de conocimientos deberá incluir los materiales, facilidades y talleres necesarios para la correcta asimilación del contenido y la generación de las destrezas necesarias en los asistentes. Esta actividad no representará costos adicionales para el SRI.
- La transferencia de conocimientos debe incluir todos los temas necesarios para que los funcionarios estén en capacidad de operar y administrar la solución adquirida por el SRI.

Soporte local

Soporte técnico local:

- Para la atención de requerimientos de soporte técnico local el contratista deberá cumplir con lo establecido en el acuerdo de nivel de servicio.
- En caso de controversia sobre la prioridad de un requerimiento de soporte técnico, prevalecerá el criterio del SRI.
- Si la atención de un requerimiento requiere el levantamiento de información, la ejecución de algún comando, la captura u obtención de datos o la obtención de registros de eventos (“logs”), es responsabilidad del contratista hacer todas las solicitudes y gestiones necesarias de forma oportuna y previsiva para obtener estos(as), sin perjuicio del cumplimiento del acuerdo de nivel de servicio.
- Las actividades necesarias para la atención de requerimientos podrán ser realizadas remota o presencialmente según lo requiera el personal técnico del SRI.
- Los horarios de trabajo se acordarán con el Administrador del Contrato.
- Todo requerimiento ingresado deberá tener un número de caso proporcionado por el contratista para poder hacer el seguimiento posterior y el contacto del especialista asignado.

- El contratista deberá suministrar el documento de Mecanismos de apertura, seguimiento y cierre de casos de soporte, donde se describa el procedimiento de ingreso, seguimiento y cierre de casos de soporte, además deberá incluir el escalamiento en niveles jerárquicos en caso de no tener respuesta de acuerdo con el SLA establecido, el escalamiento debe incluir números telefónicos y correos electrónicos de los involucrados.

Visitas Técnicas:

- Las fechas y horarios de las visitas técnicas serán previamente comunicados por el Administrador del Contrato.
- Se debe entregar un informe por cada visita técnica.

Todos los documentos que forman parte del servicio de Soporte Local deben ser entregados mediante oficio al Administrador del Contrato; así mismo todos los documentos entregados deben ser aprobados por el Administrador del Contrato.

El administrador de contrato notificará mediante oficio las fechas para las visitas técnicas con al menos 15 días hábiles de anticipación.

Acuerdo de nivel de servicio

- El tiempo de respuesta se define como el lapso entre el momento en que el SRI ingresa el requerimiento de soporte técnico por cualquier medio establecido en el instructivo entregado por el contratista, y el momento en que se inicia del análisis técnico por parte del ingeniero especialista designado a dicho requerimiento.
- La tabla de tiempos de respuesta, a continuación, establece los umbrales máximos aceptables de tiempo de espera para cada prioridad.

Prioridad	Requerimiento de soporte técnico (horas laborables)
1	1 hora
2	2 horas
3	4 horas
4	8 horas

Tabla 2. Tiempos de respuesta por prioridad.

- La tabla a continuación establece los niveles de prioridad del ACUERDO DE NIVEL DE SERVICIO:

PRIORIDAD	NIVEL DE SOPORTE	DESCRIPCIÓN
1	Crítico	Se refiere a situaciones en las que uno o varios componentes de la solución de herramienta de identidades ocasiona la indisponibilidad total del servicio.
2	Alto	Se refiere a situaciones en las que uno o varios componentes de la herramienta de gestión de identidades ocasiona la indisponibilidad parcial (de algunas funcionalidades) o degradación (lentitud, intermitencia) del servicio.
3	Medio	Se refiere a situaciones en las que uno o varios componentes de la herramienta de gestión de identidades generan errores que no afectan a la disponibilidad u operación del servicio, sin embargo, son alertas que deben ser atendidas para que a futuro no provoquen incidentes de mayor impacto.
4	Bajo	Corresponden a solicitudes de información o consultas referentes a funcionalidades de la herramienta.

Tabla 3. Descripción de los niveles de prioridad.

2.3. PRODUCTOS Y SERVICIOS ESPERADOS

LICENCIAMIENTO Y SOPORTE DE FÁBRICA

a) Características generales de aprovisionamiento de accesos	
a.1)	La herramienta debe gestionar el ciclo de vida de personas y sus identidades (cuentas) donde se permita realizar las siguientes operaciones sobre las mismas: • Creación de personas e identidades • Actualización de datos de personas e identidades • Habilitación y des habilitación de personas e identidades • Eliminación de personas e identidades
a.2)	Aprovisionamiento de identidades para 3.142 personas.
a.3)	La herramienta debe convertirse en la fuente única para la gestión de identidades del usuario y sus accesos lógicos, siendo capaz de identificar inconsistencias entre lo registrado en su base de datos y los sistemas administrados y corregir dichas inconsistencias mediante conciliaciones periódicas.
a.4)	La herramienta debe permitir la creación, actualización y eliminación de perfiles (conjunto de roles) y la asignación de uno o varios perfiles a las personas. La actualización de perfiles debe reflejarse automáticamente en las personas que tengan asignado los perfiles actualizados.
a.5)	La herramienta debe ser capaz de generar, actualizar y sincronizar las contraseñas de los sistemas administrados a través de la solución de gestión de identidades.

a.6)	La herramienta debe tener interfaces web separadas para los administradores y para los usuarios finales del sistema.
a.7)	La autenticación en la consola administrativa y de usuario debe ser integrada con Directorio Activo Microsoft (LDAP) del SRI.
a.8)	La herramienta debe estar certificada y probada en ambientes virtualizados con VMWARE ESXi versión 7.0.3 o superior, las máquinas virtuales sobre las que se instalará la solución serán proporcionadas por el SRI.
a.9)	La herramienta debe contar con los mecanismos necesarios para respaldar y restaurar la base de datos, configuración y logs, y poderlos transferir a un FTP/SFTP externo, de manera automática y calendarizada.
a.10)	La información de las personas, identidades y sus accesos, debe ser replicada automáticamente desde el ambiente de Producción hacia los ambientes de Certificación y Contingencia.
a.11)	La interfaz web de usuarios finales debe ser personalizada de acuerdo con los requerimientos funcionales definidos anexo *"Requerimiento Funcional – Gestión de Identidades"*, además de segura (HTTPS) y ser compatible con los principales navegadores (Google Chrome, Mozilla Firefox, Microsoft Edge).
a.12)	La interfaz web de administradores debe ser segura (HTTPS) y ser compatible con los principales navegadores (Google Chrome, Mozilla Firefox, Microsoft Edge).
a.13)	La interfaz web de administradores, debe soportar diferentes niveles de accesos que pueden ser configurados de manera independiente para cualquier usuario.
a.14)	La herramienta debe contar con un módulo gráfico de personalización de flujos de trabajos (workflow), en la que los administradores puedan realizar al menos pero no limitado a las siguientes modificaciones a los flujos de trabajo personalizados: • Cambiar el texto de una notificación, • Agregar, cambiar o eliminar un aprobador. • Agregar nuevas notificaciones. • Cambiar los tiempos de espera definidos en el flujo. • Algoritmo de generación de contraseñas. • Direcciones correo de los destinatarios en las notificaciones.
a.15)	La herramienta debe contar con un proceso para conciliar de manera periódica las identidades, sus atributos y los permisos registrados entre los sistemas detallados en el literal b). La solución de gestión de identidades debe ser capaz de mostrar las inconsistencias identificadas.
a.16)	La herramienta debe permitir que el usuario que creó una solicitud mediante los flujos de aprovisionamiento pueda hacer el seguimiento del estado de su solicitud a través de la interfaz web de usuarios finales, donde al menos se muestre, los datos de su solicitud, el estado, el especialista asignado, de una manera gráfica.
a.17)	La herramienta debe proveer la función de suspensión temporal de las identidades de las personas, soportando la especificación de fecha de comienzo y fin de la suspensión mediante los flujos definidos en el anexo *"Requerimiento Funcional – Gestión de Identidades"*.
a.18)	La herramienta debe permitir la delegación de aprobadores en los flujos de aprovisionamiento de forma temporal, de tal forma que el aprobador pueda especificar la fecha de comienzo y fin de la delegación.

a.19)	La herramienta debe permitir la parametrización en horas o días laborables del tiempo límite que dispone un aprobador para las tareas de aprobar/rechazar una solicitud dentro del flujo antes que se continué con la siguiente tarea o nivel de aprobación. Para esto la solución deberá permitir registrar los días feriados de cada año que serán considerados como no laborales de lunes a viernes.
a.20)	La herramienta debe permitir visualizar en forma gráfica los diferentes tipos de correlaciones existentes ente personas, sus identidades, roles / perfiles asociados.
a.21)	La herramienta debe permitir la carga masiva inicial de las personas a partir de la base de talento humano, así como las identidades de los sistemas administrados con los accesos existentes, el formato de la información se acordará con el contratista.
a.22)	La herramienta deberá detectar las discrepancias entre los accesos aprobados mediante el sistema de gestión de identidades y los accesos locales en cada sistema administrado, detectar las cuentas huérfanas y las cuentas con privilegios adicionales, que no se hayan definido mediante el sistema de gestión de identidades.
a.23)	Los flujos de trabajo deben soportar niveles de aprobación de gestión de personas y asignación de perfiles y roles de acuerdo con una estructura jerárquica tomada del Sistema de Talento Humano y con un flujo de trabajo automatizado.
a.24)	La herramienta debe permitir crear notificaciones que se envíen vía correo electrónico, las mismas que deben ser personalizables, tanto el título, cuerpo del mensaje y los destinatarios. Las notificaciones se generan al menos para: • Informar alertas • Enviar reportes. • Notificar acciones dentro de los flujos de aprovisionamiento.
a.25)	Para todos los casos en los que se requiera una intervención del usuario con el sistema, se enviará una notificación al usuario mediante correo electrónico que incluya la dirección (url) de acceso directo para gestionar dicha intervención.
a.26)	La herramienta de Identidades debe permitir al Administrador efectuar la actualización masiva de los roles / Perfiles, para esto el proveedor debe proporcionar los mecanismos necesarios para la ejecución de estas actualizaciones, según sea requerido, dentro de las funcionalidades están: • Asignación o revocatoria masiva de uno o varios roles a una o varias identidades. • Asignación o revocatoria masiva de uno o varios perfiles a una o varias personas. • Mecanismo para realizar una migración de todos los perfiles del Sistema de Gestión de Identidades que dispone actualmente el SRI de acuerdo con su codificación actual, esto incluye todos los roles definidos para cada perfil.
a.27)	La herramienta de Identidades deberá permitir a los administradores crear, eliminar o actualizar los perfiles para cada unidad administrativa.
a.28)	La herramienta deberá contar con los registros de transacciones sobre todas las acciones ejecutadas en los flujos de trabajo, o sobre cualquier objeto (personas, identidades, roles, perfiles) de tal forma que se puedan visualizar al menos los siguientes campos: • Solicitante • Para quien se solicitó la transacción • Acción solicitada

	• Roles o perfiles solicitados • Fecha y hora de ejecución de cada fase del flujo de trabajo. • Valores antes y después de información actualizada. • Administrador asignado que gestionó la solicitud. • Estado de la solicitud. • Tipo de flujo de trabajo. Se debe poder filtrar por al menos los mismos campos mencionados anteriormente.
a.29)	En el caso de que se ingrese más de una solicitud simultáneas para la misma persona, la herramienta debe contar con los mecanismos necesarios que garanticen que todas las solicitudes se ejecuten de manera exitosa sin sobre escribir los cambios generados por cada solicitud.
a.30)	Los archivos adjuntos que carguen los solicitantes en determinados flujos deben ser guardados como histórico en la herramienta y poder ser visualizados por el administrador asignado en la misma herramienta o tener la opción de descargarlos en cualquier momento.
a.31)	Las acciones de personal (APA) del sistema de talento humano, deben ser procesadas en orden ascendente de acuerdo con el campo de fecha de modificación de estas, es decir, primero las más antiguas.
a.32)	En las solicitudes de acceso no puede darse el caso que las jefaturas de las unidades administrativas puedan solicitar accesos para ellos mismos, en estos casos los debe solicitar la jefatura del siguiente nivel jerárquico.
b) Integraciones	
b.1)	Integración con el sistema Directorio Activo (LDAP) de Microsoft en versión 2019 o superior, la integración debe incluir al menos las tareas de creación y eliminación de cuentas, actualización de información de cuentas, agregar y remover cuentas en grupos de seguridad y grupos de distribución.
b.2)	La herramienta debe incluir, para todos los ambientes requeridos, las tareas de programación para el desarrollo del conector e integración con los procedimientos almacenados de la base de datos del módulo de seguridad del sistema de administración de información (ADM) que se encuentra desarrollado en: • Base de Datos Oracle 12c o superior. • Lenguaje PL / SQL La herramienta también debe incluir, para todos los ambientes requeridos, las tareas de programación para el desarrollo del conector e integración con el sistema de Talento Humano (SIGETH), mismo que será tomado como fuente autoritativa de personas, y que se encuentra desarrollado en: • Base de Datos Oracle 11c o superior. • Lenguaje PL / SQL Además, la herramienta debe incluir, para todos los ambientes requeridos, las tareas de programación para el desarrollo del conector e integración con la herramienta de

	requerimientos del SRI, mediante consumo de web services o API publicados por dicha herramienta. En total se debe desarrollar e integrar 3 conectores personalizados.
b.3)	El conector de la herramienta hacia el sistema descrito en el punto b.1) debe permitir la actualización de información de la identidad en al menos los siguientes campos: • Nombres, apellidos, cargo, cedula de identidad, departamento, unidad, agencia, correo electrónico. • Nombre de visualización. • Grupos y listas de distribución a los cuales pertenece. • Contraseña de la identidad. • Sincronización periódica y automática de los datos con el sistema administrado. • Sincronización por demanda de los datos con el sistema administrado.
b.4)	Creación, actualización, bloqueo y eliminación automática de las identidades de las personas en los sistemas descritos en los puntos b.1) y b.2) de acuerdo con la información ingresada en los flujos de aprovisionamiento incluidos en el requerimiento funcional de automatización.
b.5)	Todos los objetos relacionados a las entidades de personas, roles, perfiles, identidades, así como los registros de auditoría deben ser almacenados en una base de datos independiente a los sistemas mencionados en los puntos b.1) y b.2), se debe incluir el licenciamiento de dicha base de datos e incluir el afinamiento, configuración de respaldo y soporte de esta base de datos como parte del soporte local de la solución.
c) Certificación de accesos	
c.1)	La herramienta debe permitir generar procesos de certificación de accesos por unidad administrativa. Los parámetros incluidos en la certificación deben poder ser personalizados por el administrador.
c.2)	La herramienta debe generar un score de nivel de riesgo por cada identidad de acuerdo con reglas de negocio parametrizables y alertar en caso de sobrepasar los umbrales definidos por el administrador.
c.3)	La herramienta debe proporcionarles informes de toda la actividad del proceso de certificación para la revisión de un auditor y para cumplir con los requisitos de cumplimiento.
c.4)	La herramienta debe soportar la ejecución de múltiples certificaciones al mismo tiempo.
c.5)	La herramienta notificará automáticamente a los certificadores cuando comience el proceso y les recordará antes de que venza el plazo.
c.6)	La solución permite a los administradores guardar plantillas de certificación para uso futuro.
c.7)	La herramienta permite a los administradores guardar certificaciones para programarlas para que se ejecuten en el futuro o en forma calendarizada.
c.9)	La herramienta permite a los certificadores tomar decisiones de aprobación y revocación, y cambiar las decisiones antes de que sean enviadas.
d) Segregación de funciones	

d.1)	La herramienta debe poder crear políticas de segregación de funciones. Es decir, políticas que restringa que ciertas unidades no puedan tener asignados roles o perfiles definidos.
d.2)	La herramienta debe enviar notificaciones a los administradores cuando se descubren violaciones a las políticas de segregación.
d.3)	La herramienta debe permitir a los solicitantes ver si están enviando una solicitud de acceso que contiene violaciones de la política de segregación de funciones.
e) Registros de auditoria	
e.1)	La herramienta debe proveer al menos los siguientes registros de auditoria para ser visualizados desde una interfaz de administrador: • Solicitudes generadas automáticamente por los flujos de trabajo para creación, actualización y eliminación de identidades, y el código de la acción de personal que disparó el flujo. • Detalle de cada actividad de los flujos de trabajo, que contenga al menos, la fecha y hora de ejecución, administrador de accesos asignado a la actividad y acción del aprobador (si requiere intervención manual), resultado de cada actividad. • Solicitudes de accesos (asignación o revocatoria) con el detalle de los roles o perfiles solicitados, nombres completos y cuentas del solicitante y asignatario de dichos accesos. • Visualización de los documentos cargados por el solicitante en caso de ser solicitudes de roles críticos. • Detalle de justificación en el caso de aprobar o rechazar una solicitud de accesos y el nombre del administrador de accesos que gestionó la solicitud. • Solicitudes de conciliación con el detalle de fecha, hora y solicitante. • Solicitud de creación, actualización y eliminación de perfiles con el detalle de los roles agregados y eliminados, nombre del solicitante, código y nombre del perfil. Se requiere que todas las pistas de auditoría se almacenen en una base de datos y que tengan la facilidad de ser extraídas para procesos de control. Los reportes deben ser exportables hacia archivos con formatos: csv o txt o xml o xls.
f) Reportes	
f.1)	La herramienta debe proveer un módulo de reportes para los administradores con información detallada al menos los siguientes casos: • Reporte de ingresos, movimientos y bajas de personal ejecutados; perfiles y roles revocados • Reporte de la trazabilidad de los accesos y cuentas asignados y revocados. • Reporte de mantenimiento de perfiles (Agregados, Actualizados, Eliminados en el Sistema de Identidades), debe incluir Descripción del cambio, roles agregados o eliminados al perfil, fecha de la modificación y usuario que ingresó dicha información • Reporte de las actividades realizadas por los autorizadores en los que se incluyan:

	○ Autorizaciones/negaciones para Asignación de roles por excepción en que incluya al menos los siguientes campos: Descripción, fecha, hora, actividad, flujo relacionado. ○ Hora y fecha de las actividades ejecutadas. ○ Nombre del funcionario que ejecutó las tareas de acuerdo con los flujos. • Reporte de personas con sus identidades relacionadas en los sistemas administrados. • Reporte de estructura jerárquica de unidades administrativas del SRI. • Reporte de personas y roles/perfiles asignados por unidad administrativa. • Reporte de cuentas genéricas. • Reporte total de perfiles y los roles que contienen. • Reporte de usuarios que tengan asignado determinado rol/perfil en determinada unidad administrativa. • Reporte de solicitudes generados por/para una persona. La herramienta debe permitir la construcción de reportes personalizados con campos a escoger de acuerdo con la necesidad del SRI.
f.2)	La herramienta debe proveer al menos los siguientes reportes para ser visualizados desde una interfaz de usuario final: • Reporte de personas con sus identidades relacionadas en los sistemas administrados, por unidad administrativa. • Reporte de personas y roles/perfiles asignados por unidad administrativa. • Reporte de cuentas genéricas y sus responsables, por unidad administrativa. • Reporte de solicitudes generadas, por unidad administrativa.

IMPLEMENTACION Y TRANSFERENCIA DE CONOCIMIENTOS

g) Implementación	
g.1)	La herramienta debe ser instalada en los siguientes ambientes: • Desarrollo • Certificación • Producción • Contingencia
g.2)	La herramienta debe integrarse con los sistemas administrados indicados en el apartado b) “Integraciones”.
g.3)	Se debe implementar los flujos personalizados indicados en el Anexo *“Requerimiento Funcional – Gestión de Identidades”*.
g.4)	La implementación debe tener al menos las siguientes fases: • Desarrollo • Pruebas de certificación • Puesta en producción • Periodo de estabilización en producción

	• Entrega final en producción
h) Transferencia de conocimientos	
h.1)	Transferencia de conocimientos para al menos 8 personas con una duración de al menos 20 horas.
h.2)	La transferencia debe incluir un certificado de asistencia para cada persona.
h.3)	Material impartido en formato digital.
i) Migración de información	
i.1)	Se debe migrar todas las entidades de la herramienta actual a la nueva, de acuerdo con el siguiente detalle: • Personas • Perfiles y los roles que contiene cada uno de ellos.
i.2)	Se debe conciliar todas las cuentas de red de usuarios de Directorio Activo y de ADM para que aparezcan en la nueva herramienta de Gestión de Identidades
i.3)	Se debe generar un mecanismo para asociar masivamente cada cuenta de Directorio Activo y de ADM a la persona que le corresponde.
i.4)	Se debe migrar los perfiles asignados actualmente a las personas a la nueva herramienta.
i.5)	Se debe conciliar todos los roles de ADM para que aparezcan en la nueva herramienta de Gestión de Identidades, con todos sus datos.
i.6)	Se debe migrar la estructura jerárquica del SRI cargada en la actual herramienta a la nueva, con todos sus datos.

SOPORTE LOCAL

j) Soporte técnico local	
j.1)	Incluye asistencia ante incidentes para todos los componentes que conformen la herramienta.
j.2)	Se debe entregar un informe por cada caso reportado y solventado.
k) Visitas Técnicas	
k.1)	Se debe realizar una visita técnica semestral, donde se ejecuten al menos las siguientes actividades: • Verificar que el mecanismo de respaldos está operando correctamente. • Instalación de parches o versiones estables de software recomendados por el fabricante en todos los componentes de la herramienta. • Validar la necesidad de afinamiento de configuraciones de seguridad y de operación de la herramienta para mejorar el desempeño, de acuerdo con las recomendaciones del fabricante.

3. GLOSARIO DE TÉRMINOS TÉCNICOS

- **ADM**: Sistema de Administración de Información.
- **LDAP**: Lightweight Directory Access Protocol.
- **SIGETH**: Sistema Integrado de Gestión del Talento Humano.

- **IDENTIDAD:** Cuentas asociadas a una persona.
- **PERSONA:** Entidad donde se refiere a personas y su información laboral, sin importar si es interno, externo o pasante.
- **ROL:** Acceso específico a una parte de una aplicación.
- **PERFIL:** Conjunto de roles.
- **APA (Acción de Personal):** Documento habilitante que genera la unidad de Talento Humano para poder generar un ingreso, movimiento o baja de personal.
- **API:** Interfaz de programación de aplicación que puede ser utilizada entre sistemas para integrarse.

4. PLAZO DE EJECUCIÓN

El plazo de ejecución de este contrato será de hasta 1.109 días calendario contados a partir del día siguiente laborable de la suscripción del contrato.

Licenciamiento y soporte de fábrica

- El plazo para la activación de las licencias y soporte de fábrica de la Herramienta de Gestión de Identidades será de 15 días calendario contados a partir del día siguiente laborable de la suscripción del contrato.
- La vigencia del licenciamiento y el soporte de fábrica de la Solución de Gestión de Identidades será de 1.095 días contados a partir de la fecha de su activación.
- El plazo de entrega de la documentación correspondiente al licenciamiento y soporte de fábrica, misma que se la detalla en la metodología de trabajo será de hasta 10 días calendario contados a partir del día siguiente de la activación de la licenciamiento y soporte de fábrica.

Implementación y transferencia de conocimientos

- El plazo de entrega del plan de implementación de la Solución de Gestión de Identidades será de hasta 15 días calendario contados a partir del día siguiente laborable de la activación de las licencias.
- El plazo para la implementación de la Solución de Gestión de Identidades será de hasta 150 días calendario contados a partir del día siguiente laborable de la activación de las licencias.
- El plazo para la entrega de los documentos detallados en la metodología de trabajo relacionados a la implementación será de hasta 15 días calendario a partir del siguiente día laborable de la finalización del periodo de implementación.
- El plazo para la transferencia de conocimientos de la solución implementada y la entrega de la lista de asistentes y el material con el que se impartió la transferencia de conocimientos será de hasta 15 días calendario contados a partir del día siguiente laborable de la finalización de la implementación.

Soporte local

- El plazo de vigencia del servicio de soporte local será de 1.095 días calendario contados a

partir de la fecha de la activación de las licencias.

- El plazo de entrega de los documentos de mecanismos de apertura, seguimiento y cierre de casos con el fabricante y con el contratista será de hasta 10 días calendario contados a partir del día siguiente laborable de la entrega de las licencias.
- El plazo de entrega del informe consolidado de los casos de soporte atendidos será de hasta 10 días calendario después de finalizado cada período de soporte (anual).
- El plazo de entrega de los informes de las visitas técnicas será de hasta 10 días calendario contados a partir del día siguiente laborable de concluido la visita técnica.
- El administrador de contrato notificará mediante oficio las fechas para las visitas técnicas con al menos 15 días hábiles de anticipación.

5. FORMA Y CONDICIONES DE PAGO

Licenciamiento y soporte de fábrica: El 100% de este rubro se pagará previa presentación de la planilla de pago y el Acta de Entrega Recepción correspondiente.

- Para la suscripción del acta de entrega recepción correspondiente al licenciamiento y soporte de fábrica, el contratista deberá entregar mediante oficio dirigido al administrador del contrato, la documentación que sustente la activación del licenciamiento de la solución de gestión de identidades y de los componentes necesarios para el normal funcionamiento para las 3.142 personas y el soporte de fábrica, y se adjuntará:
  - Instructivo para abrir casos directamente con el fabricante.
  - Instructivo para abrir casos con el contratista.
  - Instructivo para acceder a la base de conocimientos del fabricante.
  - Guía de acceso y uso del portal y/o interfaz de gestión

Implementación y transferencia de conocimientos: El 100% de este rubro se pagará previa presentación de la planilla de pago y el Acta de Entrega Recepción correspondiente.

- Para la suscripción del Acta de Entrega Recepción parcial correspondiente a la Implementación y transferencia de conocimientos, el contratista deberá entregar, mediante oficio dirigido al Administrador del Contrato, la siguiente documentación:
  - Documento que ejecución y fecha de finalización de la implementación.
  - La memoria técnica de la implementación en los ambientes requeridos con el detalle de todas las actividades realizadas y el detalle de los productos implementados.
  - La lista de asistencia a la transferencia de conocimiento debidamente firmada.
  - Instructivos de usuario para cada flujo personalizado.
  - Guía de administración de la solución adquirida, donde se indique al menos los siguientes puntos:
    - Paso a paso de la ejecución de cada flujo personalizado.
    - Actividades administrativas para ejecutar periódicamente o bajo demanda en la solución.
    - Generación y construcción de reportes.

- Modificación de flujos personalizados.
- Generación de respaldos de la solución.
- Modificación de plantillas de notificaciones de correo.
- Apagado, puesta en marcha y reinicio de la solución.
- Conciliación de sistemas administrados.

Soporte Local: El pago del servicio de soporte local se realizará anualmente. Para estos pagos se requerirá la presentación de la planilla de pago y la suscripción del Acta de Entrega Recepción correspondiente.

Para la suscripción del Acta de Entrega Recepción correspondiente, el contratista deberá entregar mediante oficio al Administrador de contrato:

- Los Informes de las visitas técnicas por cada visita realizada.
- El Informe Consolidado de los casos de soporte atendidos, que contenga los siguientes campos:
  - La fecha y hora;
  - Descripción del problema o solicitud (Explicar claramente cuál es el problema o la solicitud que necesita atención. Proporcionar detalles específicos, como mensajes de error, comportamientos inesperados, etc.);
  - Prioridad y nivel de severidad;
  - Número de ticket o referencia anterior, si corresponde;
  - Los resultados de las actividades de revisión y de diagnóstico llevadas a cabo;
  - Un análisis de salud de la solución basado en la información de diagnóstico obtenida;
  - El listado de actualizaciones de software de punto final instaladas, de ser el caso;
  - Los cambios de configuración y afinamiento aplicados, de ser el caso;
  - Los hallazgos relevantes, en caso de haberlos;
  - Solución aplicada;
  - Las recomendaciones de mejora en configuración, en caso de ser necesario;

6. LUGAR DE ENTREGA

Toda documentación deberá ser entregada principalmente en formato digital, suscrita electrónicamente a la dirección de correo electrónico del administrador de contrato o a la que este defina. En los casos en que el Administrador del Contrato admita que la documentación sea diligenciada en formato físico, esta deberá entregarse en la ciudad de Quito, Av. Amazonas entre Unión Nacional de Periodistas y Pereira, Plataforma Gubernamental de Gestión Financiera, Bloque 5 (Azul), piso 1, o donde señale el Administrador del Contrato.

Las actividades del Servicio de implementación, transferencia de conocimientos y de soporte local de la solución de Gestión de Identidades deben ser entregados en la ciudad de Quito, Av. Amazonas entre Unión Nacional de Periodistas y Pereira, Plataforma Gubernamental de Gestión Financiera, Bloque 5 (Azul), piso 1. Para los casos que no se requiera intervención directa, deben ser

entregados mediante sesiones remotas supervisadas por el personal de la Coordinación de Seguridad Informática del SRI.

El Administrador del Contrato podrá realizar el cambio del lugar de entrega cuando así lo considere necesario, mediante correo electrónico dirigido al contratista.