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 LA SOLUCIÓN DATA LOSS PREVENTION**"

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 19 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					
Item	**Tipo de recurso**	**Descripción producto / servicio**	**Cantidad**	**Costo unitario**	**Costo Total**
1	Componentes de Software	Suscripciones de software DLP con soporte de fábrica por 1 año. Incluye activación de Consola de gestión y administración de la solución	3142		
	SERVICIOS CONEXOS				
2	Componentes de Software	Soporte extendido de fábrica (2 años adicionales)	2		
3	Servicios conexos	Implementación y transferencia de conocimientos	1		
4	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

Actualmente el SRI tiene en operación una base de dispositivos de punto final desplegada con diferentes versiones de Sistema Operativo de acuerdo con el siguiente detalle con corte al mes de julio de 2023.

Sistema Operativo	**Número de Dispositivos de punto final**
macOS	8
Windows 10	2.084
Windows 11	29
Windows 8.1	1.021
Total, general	**3.142**

Fuente: Consola de gestión de la solución de Antivirus institucional.

2. SERVICIOS REQUERIDOS

2.1. ALCANCE

Suscripciones y soporte de fábrica

- Suscripción tipo nube para 3.142 agentes de dispositivo de punto final que incluye el licenciamiento de técnicas avanzadas de detección y autoaprendizaje, por 1.095 días.
- Soporte de fábrica para toda la solución por 1.095 días.

Implementación y transferencia de conocimientos

- Implementación y activación de las suscripciones adquiridas por el SRI.
- Configuración de las políticas de protección.
- Implementación en sitio de los 3.142 agentes a nivel nacional, dichos componentes deberán ser desplegados en las últimas versiones liberadas por el fabricante. En el siguiente cuadro se detallan la cantidad de usuarios por agencia del SRI.

AGENCIAS SRI		
Cantón	**Ubicación**	**Usuarios**
AMBATO	AV. MANUELITA SAENZ Y FRANCISCO DE GOYA	28
AMBATO	BOLIVAR 15-60 ENTRE MARTINEZ Y LALAMA	88
AZOGUES	BARTOLOME SERRANO ENTRE BENIGNO MALO Y JULIO MARIA MATOVELLE	17
BABAHOYO	AV. ENRIQUE PONCE LUQUE Y AV. 25 DE JUNIO	39
CHONE	7 DE AGOSTO Y COLON	12
CUENCA	AV. REMIGIO CRESPO TORAL 5-28 Y LORENZO PIEDRA	141
ESMERALDAS	AV.PRINCIPAL PUERTO PESQUERO Y AV.JAIME ROLDOS AGUILERA -CAC	38
FRANCISCO DE ORELLANA	AV. 9 DE OCTUBRE Y PUTUMAYO	17
GUARANDA	GARCIA MORENO S/N Y 7 DE MAYO	17
GUAYAQUIL	AV. 9 DE OCTUBRE Y PICHINCHA, EDIFICIO CFN	13
GUAYAQUIL	AV. FRANCISCO DE ORELLANA Y JUSTINO CORNEJO	470
GUAYAQUIL	ROSA BORJA DE ICAZA Y CHAMBERS	13
IBARRA	FLORES 6-59 ENTRE BOLIVAR Y SUCRE	45
JIPIJAPA	AV. ALEJO LASCANO Y CALLE SIN NÚMERO ESQ EDIF REGISTRO CIVIL	6
LA MANA	CALLE GONZALO ALBARRACIN ENTRE MANABI Y SAN PABLO	6
LA TRONCAL	HEROES DE VERDELOMA Y AV. 25 DE AGOSTO	6
LAGO AGRIO	AV. ELOY ALFARO 908 ENTRE PROGRESO Y AV. DEL CHOFER	24
LATACUNGA	SANCHEZ DE ORELLANA 15-68 Y PADRE SALCEDO	39
LOJA	BERNARDO VALDIVIESO 8-54 ENTRE ROCAFUERTE Y 10 DE AGOSTO	88

MACAS	AV. 24 DE MAYO Y GABINO RIVADENEIRA	15
MACHALA	AV. 25 DE JUNIO KM 1 1/2 VIA A PASAJE	111
MANTA	CALLE 23 Y AV. CIRCUNVALACION BARRIO PERPETUO SOCORRO	26
MILAGRO	AV. CRISTOBAL COLON Y 17 DE SEPTIEMBRE - CAC DE MILAGRO	8
PASTAZA	9 DE OCTUBRE Y CESLAO MARIN	19
PORTOVIEJO	AV. 15 DE ABRIL Y LOS NARDOS	123
QUEVEDO	BOLIVAR Y CUARTA ESQUINA	15
QUITO	AV. AMAZONAS ENTRE UNION NACIONAL DE PERIODISTAS Y JOSE VILLALENGUA	802
QUITO	AV. RIO AMAZONAS ENTRE GENERAL ROBLES Y VICENTE RAMON ROCA	88
QUITO	AV. AMAZONAS ENTRE UNION NACIONAL DE PERIODISTAS Y JOSE VILLALENGUA	97
QUITO	AV. GALO PLAZA LASSO N58-162 Y AV. LUIS TUFIÑO	23
QUITO	AV. LUIS CORDERO 377 Y AV. GENERAL ENRIQUEZ, C.C. RIVER MALL	6
QUITO	AV. QUITUMBE ÑAN Y AV. AMARU ÑAN - PLATAFORMA GUBERNAMENTAL	18
QUITO	AV. RIO AMAZONAS ENTRE GENERAL ROBLES Y VICENTE RAMON ROCA	226
QUITO	OSWALDO GUAYASAMIN Y ARZOBISPO GONZALEZ SUAREZ -VENTURA MALL	7
QUITO	SALINAS N17-203 Y SANTIAGO	203
RIOBAMBA	PRIMERA CONSTITUYENTE Y ESPEJO	72
SAN CRISTOBAL	ALSACIO NORTHIA S/N Y MANUEL J. COBOS	5
SANTA CRUZ	SAN CRISTOBAL Y AV. BALTRA	8
SANTA ELENA	AV. 9 DE OCTUBRE 451 Y JOSUE ROBLES BODERO	20

SANTO DOMINGO	AV. QUITO 1486 Y LOS NARANJOS	45
SUCRE	AV. ROTARIA Y EUGENIO SANTOS	5
TENA	AV. 15 DE NOVIEMBRE Y DIAZ DE PINEDA	23
TULCAN	AV. CORAL S/N ENTRE PANAMA Y VENEZUELA	22
ZAMORA	AV. DEL EJERCITO Y JOSE ORELLANA	14

- Transferencia de conocimientos para 17 funcionarios del SRI.

Soporte local

- Soporte local para incidentes y requerimientos de asistencia sobre la Solución DLP por 1.095 días.
- Seis visitas técnicas para afinamiento y actualización de la Solución Data Loss Prevention (DLP) durante la vigencia del contrato.

2.2. METODOLOGÍA DE TRABAJO

Cláusulas generales

- Todas las actividades que impliquen cambios en la configuración de la Solución Data Loss Prevention (DLP) deberán ser informados al Administrador del Contrato, y deberán ser aplicados de manera controlada en coordinación con el personal del SRI.
- Durante la ejecución del contrato, si el Contratista requiere hacer algún cambio en el personal incluido en su oferta técnica, deberá notificar al Administrador de Contrato adjuntando la hoja de vida actualizada (igual o superior a lo requerido en los presentes términos de referencia) y la documentación de soporte del personal técnico que avale el cumplimiento de los perfiles establecidos. El SRI a través del Administrador de Contrato, se reserva el derecho de verificar toda la información que sea proporcionada por los oferentes del servicio.
- 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.
- Toda documentación e informes deben ser aprobados por el 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.

Suscripciones y soporte de fábrica

- Los 3.142 agentes de punto final, así como para la consola de gestión y administración de la Solución DLP deberán ser activados mediate suscripción tipo nube e incluirá el soporte de fábrica necesario para el correcto funcionamiento de la solución.
- Durante el periodo de vigencia del soporte de fábrica el SRI debe tener acceso a:
    - Nuevas versiones del sistema y actualizaciones.
    - Derecho a abrir casos con el fabricante.
    - Acceso a la base de conocimiento del fabricante.

Implementación y transferencia de conocimientos

Implementación:

- El contratista deberá entregar al Administrador del Contrato el Plan de Implementación que incluirá al menos:
    - Cronograma de trabajo.
    - Personal asignado, especialmente si los trabajos son en sitio.
- El contratista deberá desplegar en las instalaciones del SRI la totalidad de los agentes de punto final de la solución de prevención de fuga de información DLP.
- El despliegue del componente de software de punto final deberá ser realizado en su totalidad por el contratista. Se acepta la utilización de mecanismos de distribución remota de software provistos por el Contratista; sin embargo, en el caso de no contar con mecanismos de distribución remota o que estos fallen, la instalación se deberá realizar en sitio.
- Los horarios de trabajo se acordarán con el Administrador del Contrato, sin incluir costos adicionales por trabajar en fines de semana, feriados, o fuera del horario laboral.

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 Data Loss Prevention (DLP).
- Se requiere una transferencia de conocimientos especializada para diecisiete (17) funcionarios del SRI con una duración de al menos veinte horas (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 Data Loss Prevention (DLP) adquirida por el SRI.

Soporte Local

Mantenimiento Preventivo

- Cada año se deben realizar dos visitas técnicas, presencial o remota, de al menos 4 horas de duración que incluya al menos las siguientes actividades:
  - ✓ Validar el correcto funcionamiento de la Solución Data Loss Prevention (DLP);
  - ✓ Aplicar de forma controlada los afinamientos de configuración o seguridad recomendados por el fabricante;
  - ✓ Revisar los registros de eventos del sistema en busca de novedades;
  - ✓ Validar los mecanismos de generación de respaldos de configuración y registros de eventos.
  - ✓ Validar el estado de conexión y versiones de los equipos de punto final e identificar posibles problemas o equipos que requieran atención.
  - ✓ Luego de la visita técnica realizada, el proveedor deberá elaborar y presentar el Informe de Mantenimiento Preventivo en base a la información obtenida en los puntos anteriores, el mismo que debe ser entregado al Administrador del Contrato mediante oficio.
- Realizar la actualización de los equipos de punto final a la última versión recomendada por el fabricante, en coordinación con el Administrador del Contrato.
- Las fechas y horarios de los mantenimientos preventivos y actualizaciones, serán previamente comunicados por el Administrador del Contrato.

Soporte técnico

- El servicio de soporte local debe estar disponible las 24 horas del día, los 7

días de la semana, durante la vigencia del contrato, para receptar los requerimientos de asistencia técnica, conforme la sección **Acuerdo de nivel de servicio**.

- El servicio de soporte local se trabajará en base a requerimientos de asistencia (o casos de soporte), los cuales serán registrados con el contratista local para su resolución, cumpliendo con lo establecido en la sección Acuerdo de Nivel de Servicio. El administrador entregará el listado del personal que podrá abrir requerimientos de asistencia.
- Los trabajos y soporte técnicos generados por un requerimiento de asistencia podrán ser de forma remota o en sitio según sea el requerimiento expreso del SRI.
- El SRI podrá solicitar como parte del soporte local lo siguiente:
  - ✓ Solución de incidentes por errores o mal funcionamiento de la Solución DLP
  - ✓ Validar el correcto funcionamiento de la Solución DLP.
  - ✓ Verificar que el mecanismo de respaldo de políticas y el mecanismo de respaldo de configuración esté operando correctamente;
  - ✓ Aplicar los afinamientos de configuración recomendados por el fabricante o por el contratista;
  - ✓ Validar la necesidad de cambios en la configuración de la solución;
  - ✓ Revisar los registros de eventos del sistema;
  - ✓ Realizar ajustes de configuración de las políticas requeridas por el SRI
  - ✓ Realizar ajustes en la configuración de la solución y sus integraciones.
- Se aceptará el cierre de un caso o requerimiento únicamente cuando se ha aplicado una solución definitiva al evento reportado.
- Cada vez que sea requerido por el SRI el contratista deberá suministrar asistencia técnica para el afinamiento de la operación de la Solución Data Loss Prevention (DLP), así como la documentación asociada; cumpliendo con lo establecido en la sección Acuerdo de Nivel de Servicio.

El servicio de soporte local deberá incluir los siguientes entregables:

- El Contratista deberá suministrar el documento de Mecanismos de apertura, seguimiento y cierre de casos de soporte local y del fabricante, 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.
- Para la suscripción del Acta de Entrega Recepción Parcial el contratista deberá entregar mediante oficio al Administrador de contrato:
  - ✓ Los Informes de Mantenimiento Preventivo por cada mantenimiento realizado de acuerdo con lo establecido en el apartado “Mantenimiento Preventivo”
  - ✓ 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;

- 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.
- Para la atención de requerimientos, 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 incidente 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.

Una vez fenecido el plazo de ejecución del servicio de soporte local se suscribirá la correspondiente acta entrega-recepción definitiva.

<u>Acuerdo de nivel de servicio</u>

- El tiempo de respuesta se define como el lapso entre el momento en que el SRI hace el requerimiento de soporte técnico y el momento en que se inicia el análisis técnico por parte del ingeniero especialista designado a dicho requerimiento. La notificación informativa de recepción del requerimiento no

es aceptada como el inicio del análisis técnico.

- La tabla de tiempos de respuesta, a continuación, establece los umbrales máximos aceptables de tiempo de espera para cada prioridad. El tiempo de respuesta está medido en horas consecutivas salvo que se indique lo contrario.

Prioridad	Requerimiento de soporte técnico
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. Estos niveles, en cantidad y definición, pueden ser modificados durante la ejecución del contrato previa notificación por parte del Administrador de Contrato.

PRIORIDAD	NIVEL DE SOPORTE	DESCRIPCIÓN
1	Crítico	Se refiere a incidentes en las que la Solución Data Loss Prevention (DLP) está completamente inoperable o existe una fuga de información grave que podría comprometer datos altamente confidenciales o críticos para el funcionamiento de la institución.
2	Alto	Se aplica a incidentes que, aunque no sean tan urgentes como las críticas, aún tienen un impacto significativo en el funcionamiento de la institución o en la protección de datos sensibles. Puede incluir problemas recurrentes o situaciones en las que una función importante de la Solución Data Loss Prevention (DLP) no esté operativa.
3	Medio	Se refiere a incidentes que tienen un impacto moderado en la operatividad o seguridad, pero que no representan una amenaza inmediata o crítica. Pueden incluir configuraciones de políticas que

		requieren ajustes o problemas menores de rendimiento.
4	Bajo	Corresponde a incidentes menores, ajustes de configuración / políticas de la solución, o consultas que no afectan significativamente la operación o seguridad de la Solución Data Loss Prevention (DLP). Pueden ser solicitudes de información o funcionalidades adicionales que no son urgentes.

Tabla 3. Descripción de los niveles de prioridad.

2.3. PRODUCTOS Y SERVICIOS ESPERADOS

Suscripciones y soporte de fábrica

- Los 3.142 agentes de punto final, así como el módulo de gestión y administración de la Solución Data Loss Prevention (DLP) deberán ser activados mediante suscripción tipo nube e incluirá el soporte de fábrica necesario para el correcto funcionamiento de la solución.
- La solución de protección de fuga de información Data Loss Prevention (DLP) debe tener la capacidad de monitorear 3.142 dispositivos.
- La Solución Data Loss Prevention (DLP / protección de fuga de información) debe emplear algoritmos avanzados de Machine Learning e indexación, o equivalentes, con el fin de agilizar la identificación, clasificación y etiquetado de datos, además de prevenir eficazmente cualquier fuga de información.
- El componente de software de punto final deberá soportar los siguientes sistemas operativos:
  - Windows 8.1, 10, 11; o superiores
  - MacOS 10.14, 10.15, 11, o superiores
- Se incluirá soporte de fábrica por 3 años, a partir de la activación de las suscripciones de la Solución Data Loss Prevention (DLP)).
- Los componentes de la nube y de software deben operar de forma integrada y coordinada mediante un punto único de gestión en el que debe estar disponible la interfaz de usuario para la administración y el análisis, y en este también se debe realizar el procesamiento y análisis de los eventos, incidente de fuga de información.
- La Solución Data Loss Prevention (DLP) debe poder establecer una línea base de comportamiento de los usuarios en la red tecnológica sobre el cual se realiza el monitoreo mediante el análisis de varias métricas, incluyendo al menos:
  - Volumen de datos transferidos,
  - Destino de la transferencia de información,

- Horarios de los eventos,
- Tipo de archivos transferidos,
- Patrones de acceso a archivos,
- Autenticación y uso de credenciales,
- Acciones de carga y descarga de archivos,
- Actividad de impresión.

- La Solución Data Loss Prevention (DLP) debe identificar al menos los siguientes tipos de amenazas:
  - Fugas intencionadas,
  - Fugas accidentales,
  - Exfiltración de datos,
  - Mal uso de datos,
  - Identificación de prácticas que violen regulaciones y leyes de privacidad de datos,
  - Fugas a través de dispositivos externos,
  - Transferencia de datos confidenciales a través de canales de comunicación no aprobados,
  - Fugas a través de servicios en la nube,
  - Violaciones de políticas internas,
  - Patrones de comportamiento anómalos,
  - Fugas a través de redes no seguras,
  - Uso no autorizado de dispositivos,
  - Manipulación de datos: dónde se pueden almacenar los datos, cómo se deben transferir, quién puede ver cierto tipo de datos, qué tipo de datos está permitido almacenar.
- La Solución Data Loss Prevention (DLP) debe tener la capacidad de mitigar las amenazas detectadas, tomando las siguientes acciones:
  - Las acciones de bloqueo de la solución de protección de fuga de información DLP deben ser generadas con la precisión necesaria para interrumpir exclusivamente la transferencia de información que corresponde a las acciones maliciosas detectadas.
  - La solución de protección de fuga de información DLP debe tener la capacidad de realizar el bloqueo automático de las amenazas identificadas en los escenarios específicos que el personal técnico del SRI así lo establezca en la configuración.
  - Supervisar constantemente los eventos y actividades en los dispositivos y sistemas para detectar patrones, comportamientos anómalos o acciones que puedan denotar una posible fuga de datos.
  - Cuando se detecta una actividad sospechosa o una posible fuga de información, la solución de DLP debe generar notificaciones y alertas por correo electrónico para que se pueda tomar medidas adecuadas.
  - Antes de tomar medidas drásticas, como bloquear una actividad, la solución de DLP debe proporcionar información detallada sobre la

actividad sospechosa, permitiendo al usuario justificar el motivo de la acción a realizar para la transferencia de información a ejecutar.

- La Solución Data Loss Prevention (DLP) debe poder monitorear y analizar al menos las siguientes actividades u operaciones de los dispositivos:
    - Transferencia de datos,
    - Acceso a archivos y carpetas,
    - Actividad de impresión,
    - Actividad de copiado y pegado,
    - Actividad de navegación web,
    - Analizar el contenido de correos electrónicos, mensajes instantáneos y conversaciones en línea,
    - Transferencia de datos a dispositivos externos,
    - Uso de aplicaciones en la nube,
    - Actividad de autenticación,
    - Supervisar cambios en la configuración de la solución de DLP o en el software de punto final,
    - Patrones de comportamiento anómalos,
    - Transacciones financieras y de negocios,
    - Comunicaciones con fuentes externas,
    - Intentos de eludir la detección,
    - Uso de dispositivos no autorizados,
    - Compartir datos sensibles,
    - Acceso y descarga de datos.
- La Solución Data Loss Prevention (DLP) debe permitir hacer análisis retrospectivo de los incidentes en curso, de manera que se pueda visualizar los registros de eventos del dispositivo involucrado previo a presentarse un incidente.
- El acceso a la Solución Data Loss Prevention (DLP) debe ser puesto a disposición del personal del SRI para que acceda con un perfil que le permita hacer seguimiento de los eventos, configuraciones y análisis de incidentes.
- La Solución Data Loss Prevention (DLP) debe ser capaz de agrupar los eventos e incidentes de seguridad por nivel de criticidad, en base a un análisis de inteligencia artificial y de aprendizaje automático.
- La Solución Data Loss Prevention (DLP) debe ser capaz de identificar si la información trasmitida es confidencial o crítica, basándose en un método de aprendizaje automático.
- La Solución Data Loss Prevention (DLP) debe realizar un seguimiento de auditoría de todos los dispositivos que tengan instalado el software de punto final, en la red tecnológica que está monitoreando, en el que por cada dispositivo debe registrar al menos:
    - El tipo de dispositivo,
    - El hostname,
    - El sistema operativo,
    - Tipo de archivo,

- Tamaño de archivo,
- Nombre del archivo,
- Información de origen y destino de los datos copiados,
- Hora de la transferencia,
- Ubicación del archivo,
- Información del usuario,
- Tipo de acción (lectura, escritura, eliminación, etc.),
- En el caso de imprimir, indicar información de la impresora,
- Cantidad de impresiones,
- Información del sitio web,
- Detalle sobre los correos electrónicos enviados y recibidos,
- Contenido del correo electrónico y los archivos adjuntos,
- Información de la actividad en aplicaciones de mensajería instantánea,
- Información de la actividad en aplicaciones de nube,
- Eventos de autenticación,
- Cambios en la configuración del software de punto final,
- Registro de alertas y notificaciones sobre acciones tomadas como bloqueos, notificaciones a los usuarios o acciones automáticas.

- La Solución Data Loss Prevention (DLP) debe ser capaz de monitorear y analizar una amplia variedad de tipos de archivos e información estructura y no estructurada, al menos los siguientes tipos de archivos e información:
  - Documentos de textos (ejem: DOCX, PDF, TXT, RTF, etc.),
  - Hojas de cálculo (ejem: XLSX, CSV, etc.),
  - Presentaciones (ejem: PPTX, PPS, etc.),
  - Archivos comprimidos cifrados y sin cifrar (ejem: ZIP, RAR, 7z, etc.),
  - Archivos de imagen y video (ejem: JPG, PNG, MP4, AVI, etc.),
  - Archivos de audio (ejem: MP3, WAV, etc.),
  - Archivos de bases de datos (ejem: MDB, SQL, etc.),
  - Archivos de código fuente (ejem: Java, Python, etc.),
  - Archivos de diseño gráfico (ejem: PSD, AI, etc.),
  - Archivos de texto enriquecido (ejem: HTML, XML, etc.),
  - Archivos de configuración (ejem: INI, YAML, etc.),
  - Archivos de registro (ejem: LOG, etc.),
  - Información de identificación personal,
  - Información de salud,
  - Información financiera confidencial,
  - Contraseñas y credenciales,
  - Información de contribuyentes y proveedores.
- La Solución Data Loss Prevention (DLP) debe integrarse con Microsoft Active Directory 2016 o superior para enriquecer la información de usuarios involucrados en los eventos e incidentes de seguridad detectados.
- La Solución Data Loss Prevention (DLP) debe contar con al menos un API que permita la integración directa con la solución Elasticsearch. Esta

característica debe posibilitar la transferencia en tiempo real de los registros generados por la solución DLP permitiendo la explotación y visualización mediante la herramienta Kibana

Requisitos para el servicio de nube:

El servicio de nube que contempla la gestión de las licencias, así como la consola de administración de políticas y los agentes de punto final debe cumplir con los siguientes requisitos:

SEGURIDAD DE DATOS

- Cifrado en tránsito y en reposo (TLS/SSL, cifrado de disco, etc.).
- La información generada durante la vigencia del contrato será de propiedad del SRI. Al finalizar el servicio, toda la información, incluidos los logs y pistas de auditoría, será entregada al SRI.
- Garantía del fabricante indicando que la información y logs fueron borrados de la nube permanentemente una vez que el servicio terminó.
- Políticas y procedimientos de respaldo y almacenamiento redundante.

LOGS Y PISTAS DE AUDITORÍA

- Registro y gestión de logs y pistas de auditoría, sobre las actividades y transacciones efectuadas dentro del servicio o aplicación.
- Almacenamiento de los registros de auditoria durante la vigencia del contrato.

La Solución Data Loss Prevention (DPL) debe permitir obtener logs de auditoría de los eventos detectados durante el tiempo de vigencia del contrato. La herramienta debe permitir exportar los logs de auditoría en formatos csv o Excel.

CONTROL DE ACCESO

- Gestión de claves seguras y control de acceso.
- Autenticación fuerte de usuarios (autenticación multifactorial).
- Control de acceso basado en roles y políticas de autorización.
- Auditoría y registro de actividades de usuarios.

SEGURIDAD PERIMETRAL

- Detección y prevención de intrusiones (IPS).
- Firewalls y filtrado de tráfico.
- Protección contra ataques distribuidos (DDoS).
- Protección de capa 7 para aplicaciones mediante firewalls de aplicaciones (WAF).

CONTINUIDAD Y RECUPERACIÓN

- Procedimientos de recuperación ante desastres.
- Una recuperación de datos que asegure la disponibilidad y la integridad de la información en caso de pérdida, borrado o corrupción accidental o maliciosa.

MONITOREO Y DETECCIÓN

- Monitoreo constante de eventos de seguridad y actividad anómala.
- Herramientas de análisis de seguridad y correlación de eventos.

- Automatización que permita detectar y responder a las amenazas en la nube de forma rápida y eficaz.

ACTUALIZACIONES Y PARCHES

- Proceso de gestión de vulnerabilidades.
- Políticas de actualización y aplicación de parches.

SEGREGACIÓN DE DATOS

- Aislamiento lógico de datos entre clientes.

GESTIÓN DE INCIDENTES

- Planes y procesos para la notificación y gestión de incidentes de seguridad.
- Transparencia y auditoría que permita al cliente acceder a los registros e informes sobre las actividades y los incidentes de seguridad que afecten al servicio de nube.

Implementación y transferencia de conocimientos

- Implementación de la totalidad de agentes de punto final de la solución de prevención de fuga de información DLP.
- Configuración de las políticas de protección. Estas políticas serán otorgadas por el SRI. La solución debe permitir configurar políticas de protección para bloquear o registrar la salida de información por los siguientes medios:
    - Unidades de disco externo USB
    - Unidades de CD externas.
    - Carga de archivos en sitios de almacenamiento en la nube y repositorios de compartición de archivos.
- La configuración de la solución incluye al menos los siguientes puntos:
    - Al menos 10 políticas de protección.
    - Configurar un set de palabras y caracteres clave que permitan identificar el tipo de información en documentos para las diferentes categorías definidas por el SRI.
    - Configurar un conjunto de archivos tipo, con el fin de que sirvan como insumo para los procesos de reconocimiento automáticos de la herramienta.

- Transferencia de conocimientos especializada para diecisiete (17) funcionarios del SRI con una duración de al menos veinte horas (20) horas.

3. 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 suscripciones y soporte de fábrica de la Solución Data Loss Prevention (DLP), será de 15 días calendario contados a partir del día siguiente laborable de la suscripción del contrato.
- La vigencia de las suscripciones y el soporte de fábrica de la Solución Data Loss Prevention (DLP) será de 1095 días contados a partir de la fecha de su activación.
- El plazo de entrega de la documentación correspondiente a las suscripciones y soporte de fábrica será de hasta 10 días laborables contados a partir del día siguiente laborable de la activación de las suscripciones y soporte de fábrica.

Implementación y transferencia de conocimientos

- El plazo de entrega del Plan de Implementación será de hasta 10 días laborables contados a partir del día siguiente laborable de la activación de las suscripciones.
- El plazo para la implementación de la Solución Data Loss Prevention (DLP) y la transferencia de conocimiento será de hasta 145 días calendario contados a partir del día siguiente laborable de la activación de las suscripciones.
- El plazo de entrega de la documentación correspondiente a la implementación y transferencia de conocimientos será de hasta 10 días laborables, contados a partir del día siguiente laborable de la finalización de la implementación y transferencia de conocimiento.

Soporte local

- El plazo de vigencia del servicio de soporte local será de 1.095 días contados a partir de la fecha de la activación de las suscripciones.
- El plazo de entrega del procedimiento de apertura, seguimiento y cierre de casos de soporte local y del fabricante será de hasta 10 días laborables contados a partir del día siguiente laborable de la activación de las suscripciones.
- El plazo de entrega del informe consolidado de los casos de soporte atendidos será de hasta 10 días hábiles después de finalizado cada período de soporte (anual).
- El plazo de entrega de los informes de mantenimiento preventivo será de hasta 10 días laborables contados a partir del día siguiente de concluido el mantenimiento.

4. FORMA Y CONDICIONES DE PAGO

- **Suscripciones y soporte de fábrica:** El 100% de este rubro se pagará previa presentación de la documentación que sustente la activación de las suscripciones de la Solución DLP y soporte de fábrica, la guía de acceso y uso del portal y/o interfaz de gestión, la guía de escalamiento de casos con el fabricante la planilla de pago y el Acta de Entrega Recepción correspondiente.

- **Implementación y transferencia de conocimientos:** El 100% de este rubro se pagará previa presentación de la memoria técnica de la implementación con el detalle de todas las actividades y productos ejecutados, la lista de asistencia a la transferencia de conocimiento debidamente firmada, la planilla de pago y el Acta de Entrega Recepción correspondiente.

- **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.

5. 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 herramienta DLP 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 del SRI. En caso de ser necesario, la implementación o soporte de agentes de puntos finales se los podrá realizar en sitio con base al listado de agencias 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.