Informe de estudios previos
Para la renovación del derecho de uso soporte plataforma IMPERVA

La administración pública, con el objetivo de cumplir con las funciones esenciales del Estado, lleva a cabo la actividad contractual, lo que hace trascendental la etapa precontractual. En esta etapa se realizan todas las actuaciones previas a la formalización del contrato, que incluyen las fases de planificación y preparación, entre otras, de conformidad con el artículo 62 y siguientes del Reglamento de aplicación de la Ley 340-06. Esto tiene como finalidad garantizar la correcta ejecución de los procesos de selección, un mejor aprovechamiento de los recursos y una mayor eficiencia en la ejecución de los contratos.

Dentro de la fase de planificación y preparación, se establece que todo procedimiento de contratación debe estar sustentado en estudios previos, de conformidad con políticas, manuales, guías u orientaciones normativas dictadas por la Dirección General de Contrataciones Públicas o las regulaciones especiales aplicables al objeto contractual.

El objetivo del presente informe es presentar los resultados de los estudios previos realizados por el Departamento de Gestión Seguridad de la Información, de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad que serán el punto de partida para el diseño del procedimiento a realizarse para la adquisición del servicio de **renovación derecho de uso soporte plataforma IMPERVA**, en cumplimiento con lo establecido en la Ley 340-06 y su Reglamento de aplicación aprobado mediante el Decreto No. 416-23, así como el Manual General de Procedimiento por Excepción de Contratación Pública, aprobado por la Dirección General de Contrataciones Públicas.

En este sentido, se pretende definir de forma detallada la necesidad a atender, el objeto del contrato, sus características y especificaciones técnicas, así como las particularidades del mercado, el costo estimado y otros aspectos mínimos que deben determinarse respetando los principios de igualdad y libre competencia, para el correcto diseño del procedimiento que será realizado por la entidad para satisfacer la necesidad y lograr los objetivos propuestos.

Luego de varias gestiones de levantamiento de información y consultas de las informaciones disponibles, del análisis del proceso anterior y de la validación de las condiciones de disponibilidad de dichos servicios y productos en el mercado, así como del análisis de la necesidad que se pretende satisfacer, presentamos a continuación los siguientes resultados.

Identificación de la necesidad y justificación del proceso

La Tesorería de la Seguridad Social (TSS) es una entidad autónoma y descentralizada del Estado, adscrita al Ministerio de Trabajo, dotada de personalidad jurídica y patrimonio propio, conforme el Artículo 28 de la Ley 87-01 crea el Sistema Dominicano de Seguridad Social (SDSS) modificada por la Ley 13-20 que fortalece la Tesorería de la Seguridad Social (TSS) y la Dirección General de Información y Defensa del Afiliado (DIDA).

La Tesorería de la Seguridad Social (TSS) desempeña un papel fundamental en la gestión eficiente de los recursos destinados a garantizar la seguridad y bienestar de la población y tiene a su cargo el proceso de recaudo, distribución y pago de las cotizaciones del Sistema Dominicano de Seguridad Social (SDSS), así como del Sistema Único de Información y Recaudo (SUIR).

La Tesorería de la Seguridad Social definió en su Plan Estratégico Institucional 2021-2024 los siguientes ejes estratégicos: fortalecimiento institucional, crecimiento y desarrollo y Experiencia del Usuario. Dentro de cada uno de estos ejes, se contemplan acciones que van encaminadas a la protección de los datos e informaciones, así como también al cumplimiento de todas las normativas vigentes en la legislación nacional. Dentro del Fortalecimiento Institucional, se despliegan actividades que van encaminadas al cumplimiento de los objetivos de la institución, entre ellas, una propuesta que solvente la necesidad de obtener seguridad y protección para las bases de datos críticas y, por consiguiente, agregar una capa de protección robusta que garantice auditoría sobre las mismas.

Atendiendo a lo anterior, la adquisición del servicio **Renovación derecho de uso soporte plataforma IMPERVA** permitirá a la institución: 1-Realizar una auditoría continua y en tiempo real de las operaciones en bases de datos; 2-Monitorizar usuarios con y sin privilegios; 3-Emitir alertas sobre fugas de información; 4-Facilitar la investigación forense; 5-Identificar patrones de acceso no autorizado y actividades fraudulentas; 6-Bloquear ataques en tiempo real y asegurar el cumplimiento de directivas de seguridad; 7-Detectar automáticamente sistemas de bases de datos, evaluar y parchear vulnerabilidades; 8-Controlar eficazmente los derechos de usuario;9-extender sus capacidades a servidores host, entre otras.

Identificación del objeto del contrato, su naturaleza, características y sus especificaciones

Se requiere adquirir el servicio **Renovación derecho de uso soporte plataforma IMPERVA** para la Tesorería de la Seguridad Social, cuyas oficinas principales está ubicada en la avenida Tiradentes número 33, Ensanche Naco, de esta ciudad de Santo Domingo, Distrito Nacional.

Ítem	Rubro	Descripción	Cantidad	Unidad de medida	Especificaciones
1	**81112501**	**Renovación de derecho de uso soporte plataforma IMPERVA**	1	Año	Ver detalles debajo

Las especificaciones técnicas del servicio se establecen a continuación:

1. **Condiciones Generales.**

1.1. La solución Database Activity Monitoring (DAM) / DBF (Database Firewall) ofertada debe tener la capacidad de capturar todas las acciones de usuario relacionadas con las bases de datos por el periodo de 1 año. Estas acciones se deben capturar sin requerir mecanismos propios-nativos de las bases de datos. Los motores que debe soportar la solución deben ser por lo menos los siguientes:

- Amazon Aurora MySQL - Amazon Redshift
- Amazon RDS for MariaDB Server - Amazon RDS for Microsoft SQL Server
- Amazon RDS for Oracle - Amazon RDS for PostgreSQL
- Azure SQL Server - Cloudera Data Platform (CDP)
- Cloudera Hadoop (CDH) - Couchbase Server

- Datastax Cassandra - Google Cloud MySQL
- Google Cloud SQL Server - Hortonworks Hadoop (HDP)
- IBM Db2 for i - IBM Db2 for LUW
- IBM Db2 for z/OS - IBM Information Management System (IMS)
- IBM Integrated Analytics System (IIAS) - IBM PureData System for Analytics (Netezza)
- Informix - MariaDB Server
- MarkLogic - Microsoft SQL Server
- MySQL - Oracle
- Pivotal Greenplum Database - PostgreSQL
- PostgreSQL On-Prem - SAP-HANA
- Sybase ASE - Sybase IQ
- Sybase SQL Anywhere - Teradata

1.2. La solución ofertada debe contar con el correspondiente respaldo del fabricante, para los servicios de garantía de hardware (si aplica), mantenimiento software y soporte técnico.

1.3. El fabricante de la solución deberá contar con un centro de investigación que se encargue de generar mecanismos de detección de ataques hacia las BD y de cumplimiento de estándares de seguridad y auditoría de la industria; estos mecanismos podrán ser firmas, políticas, vulnerabilidades, plantillas, entre otros. Dicho contenido deberá ser descargable de forma periódica por la solución para incrementar su capacidad de detección y mitigación de amenazas y cumplimiento.

2. Integración

2.1. La solución debe soportar el protocolo de gestión de red SNMP para ser monitoreados por las herramientas de terceros.

2.2. El sistema debe permitir la integración y envío de alertas a terceros u herramientas de correlación (SIEM) a través de syslog.

3. Monitoreo

3.1. La solución deberá incluir agentes livianos de software para monitoreo de actividad sobre el servidor, sin depender de auditoría nativa de las bases de datos o logs propios de los motores de Base de datos. Asimismo, la solución no deberá depender únicamente de dichos agentes para poder protegerlos y/o monitorearlos.

3.2. Los agentes deberán poder desactivarse si superan determinado umbral del consumo de CPU del servidor donde se encuentra instalado. Asimismo, para mejorar el performance, el agente podrá contar con políticas que permitan excluir determinados

eventos (incluyendo procesos confiables del servidor de BD y/o eventos originados a partir de una IP determinada).

3.3. Los agentes deben soportar al menos los siguientes sistemas operativos: Solaris, Microsoft Windows, Oracle_Linux, Ubuntu en sus versiones funcionales y actualizadas.

3.4. Deberá registrar todas las pistas de auditoría de manera detallada de todas las actividades referentes a las bases de datos, que permita conocer por cada transacción "quién, qué, dónde, cuándo y cómo".

3.5. La solución deberá implementar un monitoreo efectivo de usuarios privilegiados (DBA, super usuarios, desarrolladores, etc.).

3.6. La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.

3.7. La solución deberá monitorear tanto el tráfico local y el remoto de las bases de datos.

3.8. La solución deberá ofrecer la posibilidad de auditar las sesiones de base de datos. La auditoría debe incluir los siguientes datos:

- Fecha y hora de la ocurrencia del evento.
- Información de usuario de base de datos.
- Información de los objetos de bases de datos (tablas, vistas, vistas materializadas, store procedures, entre otros.) consultados/modificado y los datos consultados (resultados de la consulta).
- Instancia, esquema, base de datos, objeto y operación realizada.
- Debe mostrar las variables bind en caso de que éstas sean utilizadas por la aplicación.

3.9. La solución deberá manejar funcionalidades tan amplias o granulares como se requieran, que deberán poder ser construidas manualmente. Los criterios deberán poder usarse varios a la vez y en diferentes combinaciones de ellos:

- Tipo de datos accedido.
- Acceso a datos marcados como sensibles.
- Base de Datos, Schema, Instancia, Tabla y Columna accedido.
- Estado de autenticación de la sesión.
- Usuario y/o Grupo de Usuarios de Base de Datos conectado.
- Logins, Logouts, Queries.
- IPs de origen y destino.
- Nombre de Host origen.
- Aplicación usada para la conexión a la base de datos.
- Tiempo de respuesta/procesamiento del query.
- Número de ocurrencias en intervalos de tiempo definidos.
- Por operaciones básicas (Select, Insert, Update, Delete).
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Restore).
- Por Stored Procedure o Function utilizada.
- Hora del Día.

3.10. La solución deberá soportar la importación de certificados en formato PKCS12 y PEM.

3.11. Por cada política de auditoría se podrá especificar una cuota de espacio en disco para almacenamiento de eventos, de tal forma que las políticas consideradas críticas puedan tener mayor espacio de almacenamiento que otras políticas no críticas.

3.12. Por cada política de auditoría se podrá determinar si los logs de transacciones SQL serán respaldados en un servidor externo (FTP o SCP), indicando una frecuencia de respaldo automático.

3.13. Por cada política de auditoría se podrá definir si la solución también tendrá la capacidad de almacenar los logs de respuesta de la BD al hacer una consulta a una tabla (SELECT).

3.14. La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema, entre otras; hacia otras herramientas de administración por medio de protocolos SNMP y SYSLOG.

4. Agente

4.1. La solución, para efectos de obtener los registros de auditoría de las transacciones de BD no deberá requerir ningún cambio en la configuración o contenido de la base de datos. Esto incluye:

- Creación de usuarios en las bases de datos.
- Modificación de los permisos de los usuarios existentes.

5. Perfilamiento

5.1. La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana. El proceso deberá ser constante y deberá aprender la estructura de las bases de datos, incluyendo bases de datos, tablas, aplicaciones, IP origen, querys, así como el comportamiento de cada usuario; todo esto para el establecimiento de una línea base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.

6. Descubrimiento

6.1. La solución deberá realizar descubrimientos automatizados (escaneos) en la red para identificar servidores bases de datos ya sea a nivel de servidor o puertos habilitados.

6.2. La solución deberá tener la capacidad de descubrir y clasificar información sensible dentro de las tablas de bases de datos de acuerdo con las políticas de negocio. Las definiciones de que se considera información sensible deberán poder crearse de manera flexible y granular.

7. Análisis de vulnerabilidades

7.1. La solución deberá poder realizar escaneos a las bases de datos en diferentes niveles/capas, según lo siguiente:

- Brindar un puntaje de los riesgos e indicar cómo mitigar esos riesgos.
- Escaneo de vulnerabilidades de la base de datos y configuraciones erróneas, como contraseñas predeterminadas.
- Escaneo de cumplimiento de estándares de benchmarks o hardening como CIS y DISA-STIG.

7.2. El análisis de vulnerabilidades no debe requerir la instalación de software en el servidor de la base de datos.

7.3. La solución deberá contar con un dashboard que permita comparar una tarea de escaneo de vulnerabilidades actual con uno anterior, para verificar si las vulnerabilidades o configuraciones erróneas han sido solucionadas.

8. Control de permisos de usuarios

8.1. Deberá contar con la funcionalidad de (mediante escaneos) poder realizar informes sobre:

- Permisos efectivos de los usuarios sobre los distintos objetos de las bases de datos.
- Detección de usuarios "Dormant" o en desuso y cuáles de ellos están o no bloqueados.
- Cadenas de autorización que permiten que cierto usuario (a través de ciertos roles) tenga un permiso específico.
- Relacionar un permiso otorgado a cierto usuario con quién lo otorgó (Grantee).

9. Bloqueo

9.1. La funcionalidad de Bloqueo deberá estar activa en el mismo equipo que realiza el monitoreo de actividad de la base de datos (DAM).

9.2. De acuerdo con la detección de ataque debe permitir tomar diferentes acciones:

- Bloqueo de comando SQL.
- Bloqueo de la dirección IP correspondiente a la petición, durante una cantidad de tiempo definible.

9.3. La funcionalidad de Bloqueo no deberá depender de la funcionalidad de auditoría, es decir, se podrá implementar una política de Bloqueo para determinada transacción SQL, independientemente si dicha transacción SQL tiene una política de auditoría asociada.

10. Seguridad

10.1. La solución deberá proveer detalles sobre alertas generadas y deberá tener la facilidad de modificar las políticas asociadas desde las alertas.

10.2. Deberá poder alertar en tiempo real peticiones a la base de datos dependiendo de:

- Usuarios de bases de datos, Usuarios de Sistema operativo, IP y nombre de host de origen, binario o programa utilizado para conectarse.

- Base de datos, tabla, stored procedure, esquema.
- Tablas, esquemas, columnas.
- Operaciones realizadas (DELETE, UPDATE, GRANT, ALTER, etc.).
- Horarios de ejecución de operaciones.
- Cantidad de registros devueltos en un query y tiempo de respuesta.

10.3. La solución deberá detectar anomalías y abusos a los protocolos de red, malformaciones en los protocolos SQL y firmas de ataque conocidas destinadas a los servidores protegidos.

10.4. La solución debe detectar los siguientes eventos de seguridad:

- Acceso de usuario desconocido.
- Acceso de aplicación de base de datos desconocida.
- Acceso de cliente (origen IP) desconocido.
- Intento de ejecución de inyección de comandos SQL.
- Ejecución de un Stored Procedure desconocido.
- Acceso a una base de datos y o esquema no autorizado.
- Acceso a bases de datos, esquemas o tablas previamente definidas.
- Ejecución de comandos privilegiados (DDL).
- Ejecución de comandos SQL no autorizados.

10.5. La solución deberá examinar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son ataques complejos intentando vulnerar las aplicaciones.

11. Administración

11.1. La solución deberá ser administrada desde una sola consola (centralizada) WEB que permita la gestión de las políticas (auditoría y seguridad), informes, reportes, revisión de auditoría, monitoreo, eventos de seguridad, gestión de los distintos componentes de la solución y el monitoreo de su estado y performance.

11.2. La solución debe incluir un servidor central de administración en el cual residan el software de administración y registro de eventos generados por los diferentes componentes de la solución.

11.3. La solución deberá permitir realizar backups periódicos en forma automática de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los módulos administrados y tener la capacidad de transferirlos automáticamente a un servidor remoto utilizando los protocolos SCP y FTP. El backup deberá estar cifrado. La periodicidad de los backups se debe poder establecer desde la consola de administración.

11.4. Toda la configuración, administración y monitoreo de la solución se efectuará a través de la consola de administración.

11.5. La solución de administración debe permitir asignación de perfiles de administración por usuarios y estos perfiles deben permitir separar roles de administración y monitoreo.

11.6. Deberá permitir la definición de roles de usuarios de forma granular, de tal forma que un rol tenga acceso a determinadas vistas o menus de la solución.

11.7. Proporcionar una vista centralizada de los logs, entendiendo como tal, la unificación de los logs de la totalidad de los componentes que conforman la solución.

11.8. La solución deberá realizar detección y análisis sobre todo el tráfico en tiempo real, sin necesidad de crear un archivo log primero para su análisis posterior.

11.9. La solución de administración permitirá, como mínimo, lo siguiente:

- Agregar, eliminar o modificar la configuración en un entorno gráfico.
- Modificar las reglas de los diferentes equipos.
- Efectuar la configuración de los componentes de la solución.
- Visualizar los registros de auditoría, alertas de seguridad y eventos del sistema.
- Generar reportes ajustables por el usuario.

11.10. Permitir la generación de reportes, de toda la actividad registrada en los logs, en los formatos PDF y CSV.

11.11. Permitir la elección de información a ser incluida en los reportes de forma granular, con la capacidad de elegir las columnas a mostrar en los reportes y filtrar la información a ser mostrada. Asimismo, permitir diagramas ejecutivos de barra o pie en los reportes PDF.

11.12. Capacidad de automatizar la generación de reportes y su posterior remisión por email.

12. Data Risk Analitics

12.1. La solución debe contar con un mecanismo de inteligencia artificial que detecte usuarios comprometidos cuyas credenciales son robadas o que, sin saberlo, introducen malware en la institución.

12.2. La solución debe contar con un mecanismo de inteligencia artificial que detecte Usuarios malintencionados que deliberadamente roban o manipulan activos corporativos

12.3. La solución debe contar con un mecanismo de inteligencia artificial que detecte Usuarios descuidados que inadvertidamente ponen en riesgo datos confidenciales.

12.4. La solución debe contar con un mecanismo de inteligencia artificial que aprenda dinámicamente los patrones normales de acceso a los datos de los usuarios y luego

identifique la actividad de acceso inapropiada o abusiva para alertar de manera proactiva a los equipos de TI sobre comportamientos peligrosos.

12.5. El mecanismo de analítica debe tener la capacidad de agregar patrones de comportamiento en listas blancas, por tiempos determinados para que no se emitan alertas o se generen incidentes que coincidan por el periodo establecido.

12.6. El mecanismo de analítica debe tener la capacidad de dar visibilidad ante por lo menos los siguientes eventos:

- Modificaciones a las auditorías nativas con la intención de eliminar rastro de actividades maliciosas.
- Intento de ejecución de comandos de sistema operativo aprovechando alguna vulnerabilidad en la base de datos.
- Intento de robo de credenciales de las bases de datos consultando la metadata de las mismas.
- Exfiltración de datos.
- Modificación de la configuración o inclusión de elementos dentro de la base de datos que permitan vulnerar/atacar la información.
- Inclusión de código binario (malware) en los motores de bases de datos con el objetivo de atacar o correr código arbitrario con funciones diferentes a las autorizadas.
- Ataques que aprovechando vulnerabilidades de las bases de datos hayan logrado o hayan intentado leer archivos propios del sistema operativo.
- Un usuario malintencionado ataca la base de datos e intenta explotar una vulnerabilidad o una característica de la base de datos para obtener privilegios elevados sobre recursos y / o datos.
- Un usuario malintencionado ataca la base de datos y realiza una secuencia sospechosa que se identifica como una campaña de Ransomware.
- Se utiliza una cuenta para acceder a la base de datos en un momento atípico para un usuario y su grupo de pares.
- Un usuario interactivo (humano) está utilizando una cuenta de servicio para acceder a la base de datos.
- Una persona consulta registros en exceso de lo que normalmente consulta el, su grupo de pares y la organización.
- Un usuario no ha podido iniciar sesión satisfactoriamente más veces de lo habitual para este propietario de cuenta en particular.
- Un usuario no pudo iniciar sesión (satisfactoriamente) en la base de datos desde un servidor de aplicaciones.

- Un usuario ha intentado acceder a una cantidad anormalmente alta de bases de datos diferentes durante un corto período de tiempo.
- Un usuario inició sesión en el dispositivo corporativo de otro empleado para acceder a una base de datos.
- Un usuario interactivo (humano) accede directamente a datos comerciales a los que normalmente solo se debe acceder a través de una aplicación.
- Un usuario realizó un comando que es de naturaleza altamente sospechosa y se ejecutó de una manera anormal.
- Un usuario interactivo (humano) ha consultado una base de datos utilizando consultas SQL dinámicas de forma anormal.
- Un usuario interactivo (humano) ha escaneado tablas sensibles del sistema en varias bases de datos durante un período de tiempo relativamente corto de forma anormal.

13. Requisitos de los oferentes

13.1. El oferente debe ser una empresa consolidada en el mercado con más de 10 años experiencia en el área de ciberseguridad.

13.2. El oferente debe tener personal técnico mínimo tres (3) con certificación vigente del fabricante que garantice conocimiento para participar en cualquier etapa del ciclo de vida de la solución ofertada, debe incluirse la documentación correspondiente junto con el currículo del personal asignado de al menos tres (3) personas.

13.3. El oferente deberá debe poseer un nivel de Partner Support.

13.4. El oferente deberá demostrar poseer una alianza estratégica con una entidad internacional, que certifique exclusivamente la Seguridad de la Información, mediante un programa integral de evaluación y certificación continuo en el tiempo, demostrable a través de una carta de dicho ente internacional.

13.5. Debe poseer un centro de Operaciones de Seguridad (SOC) formalmente constituido, dónde se ejecuten todo el monitoreo, análisis de riesgo total de las soluciones bridadas u otras relacionadas. Para cumplir con este punto deberá presentar declaración jurada que así lo indique. Es importante mencionar que una mesa de ayuda o un NOC no son considerados Centro de Operaciones de Seguridad. Para cumplir con este punto deberá presentar declaración jurada que así lo indique.

13.6. La empresa que podrán aportar su conocimiento técnico para la ejecución contractual debe contar con al menos 5 años de experiencia verificable en el campo sobre el cual se presenta oferta. Para verificación de este punto debe aportar al menos tres (3) cartas firmadas digitalmente o presentar listado de referencias en formato "pdf" de clientes, a los cuales brinda servicios del mismo tipo correspondientes al objeto de esta

contratación. El listado debe tener detalle del nombre del cliente información del contacto (nombre, correo, número telefónico).

13.7. El oferente debe estar considerado líder como empresa consultora de servicios de ciberseguridad por analistas de mercado como Gartner, Forrester, IDC o Frost & Sullivan.

13.8. Para garantizar las mejores prácticas de TIC, se requiere que el oferente cuente con al menos tres (3) profesionales certificados en ITIL.

13.9. Para garantizar el apropiado cumplimiento de normas internas, mejores prácticas en TI y Seguridad Informática se requiere que el oferente cuente con al menos:

- Un (1) gestor de proyecto certificado como PMP Project Management Professional) emitida por el PMI (Project Management Institute) con más de 2 años de experiencia. Para lo cual deberá presentar documento donde conste dicha condición y su vigencia.
- Dos (2) profesionales certificados como ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (SGSI). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición.
- Dos (2) profesionales certificados en ISO/IEC 27032 Cybersecurity Manager. Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dichacondición.
- Dos (2) profesionales certificados como Certified Information Systems Security Professional(CISSP). Para lo cual deberá presentar documento donde conste dicha condición y se indique la vigencia de dicha condición.

Las particularidades del mercado, en cuanto a cómo y en cuáles plazos se ofrece ese bien, se presta el servicio

Los bienes y servicios requeridos por la entidad contratante se encuentran disponibles en el mercado local, y es ofrecido por proveedores que pueden ser personas físicas y jurídicas a nivel nacional, sin mayores complicaciones a la hora de prestarlo y el acceso a los materiales necesarios y vías de transmisión efectivas para la correcta ejecución de los servicios que se pretenden contratar. En este caso particular, se requiere que el oferente presente un cronograma que establezca claramente los plazos y las actividades a desarrollar, incluyendo fecha de inicio, implementación y entrega del licenciamiento, los cuales no podrán exceder en su totalidad los treinta (30) días hábiles, con posterioridad a la certificación del contrato por la Contraloría General de la República; la vigencia de las licencias será de un (1) año, a partir de la entrega y recibido conforme por parte del **Departamento de Gestión de Seguridad de la Información de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad.**

Asimismo, se ha determinado que se necesita soporte por un periodo de un (1) año a partir de la entrega de las licencias.

Análisis de oferta y demanda de los bienes y servicios requeridos

Hemos identificado que en el mercado existen tres (3) proveedores que se encuentran registrados en el programa de canales de Imperva y están autorizados para la comercialización de las soluciones del portafolio de Imperva en el territorio de la República Dominicana, cuales son: **Infosec Latin America, Inc. (Sistemas Aplicativos)**, **Integraciones Tecnológicas M&A, SRL** y **Multicómputos, SRL**, conforme Certificación emitida por Thales Group, empresa que tiene los

derechos sobre todos los servicios de Imperva y por lo tanto se encuentra en la facultad de emitir certificación sobre los proveedores autorizados. Ver imagen:

11 de Octubre de 2024

Atención Sres. Tesorería de la Seguridad Social (TSS)
Ref.: Canales autorizados

Por medio de la presente hago de su conocimiento un listado de 3 canales que al día de hoy se encuentran registrados en el programa de canales de Imperva y están autorizados para la comercialización de las soluciones del portafolio de Imperva en el territorio de Republica Dominicana.

- Sistemas Aplicativos
- Multicomputos
- Integratec

Sin más por el momento, quedo atento a cualquier comentario.

Esta certificación cuenta con una vigencia de 30 días a partir de su fecha de emisión

Atentamente,

Luis E. Hernandez
Channel Manager
Central America & Caribbean
Cloud Protection & Licensing
M: +52 55 4494 8849
luis-e.hernandez@thalesgroup.com

En consecuencia, resulta prudente establecer la modalidad del procedimiento como Excepción por Selección Competitiva por exclusividad, conforme lo establecido en el Artículo 54 del Decreto 416-23 que establece el Reglamento de Aplicación de la Ley 340-06: "***Artículo 54. Procedimiento de excepción por exclusividad***. *Se utilizará el procedimiento de excepción por exclusividad para obtener bienes o servicios que por su especialidad solo pueden ser suplidos por un número limitado de proveedores que pueden atender al requerimiento, que en ningún caso podrá ser mayor de cinco (5). Los oferentes que poseen la exclusividad deben demostrarlo mediante una acreditación o certificación, en caso de que la hubiere, que puede ser nacional o internacional, emitida por una persona, institución u organismo público o privado con autoridad para hacerlo.*"

Condiciones de pago

La entidad contratante procederá a realizar un primer pago correspondiente al Anticipo, el cual será del veinte por ciento (20%), del valor del Contrato y este pago se hará en un plazo no mayor de treinta (30) días hábiles a partir de la firma del Contrato y contra presentación de una Póliza de Seguro o Garantía Bancaria que cubra la totalidad del Avance Inicial.

Se realizará un segundo pago correspondiente al sesenta por ciento (60%) del monto total adjudicado, luego de la entrega de las licencias y culminado el proceso de implementación, con posterioridad a la entrega del recibido conforme por parte del Departamento de Gestión de Seguridad de la Información, en un plazo no mayor a treinta (30) días hábiles a partir del vencimiento de la factura con Comprobante Gubernamental.

Un tercer y último pago, correspondiente al restante veinte por ciento (20%) del valor del Contrato y este pago se hará en un plazo no mayor de treinta (30) días hábiles con posterioridad a la entrega y recibido conforme de los servicios profesionales accesorios a las licencias.

En ningún caso, está permitido que el proveedor reciba el pago total del servicio sin que el objeto del contrato se haya cumplido.

Unidad coordinadora del contrato

Por parte de la entidad contratante, la unidad coordinadora y ejecutora encargada del gerenciamiento del contrato será el **Departamento de Gestión de Seguridad de la Información**, **de la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad** bajo la responsabilidad del Sr. **Ly Mendez Vasquez,** encargado del referido Departamento.

El costo estimado del bien, obra o servicio a contratar, que determine el presupuesto de la contratación e identifique la partida presupuestaria a afectar.

El costo aproximado para la adquisición del servicio **renovación derecho de uso soporte plataforma IMPERVA** es **RD$9,600.000.00,** en cuya virtud, la forma idónea para satisfacer la necesidad es mediante un proceso de compras por Excepción por Selección Competitiva por Exclusividad, tomando en consideración el monto estimado y los umbrales para el 2024, aprobados por la Dirección General de Contrataciones Públicas.

Nota: Este bien y sus servicios accesorios no se encuentran sujetos al pago de impuestos. Conforme al Reglamento 293-11, de fecha doce (12) del mes de mayo del año dos mil once (2011), de la Dirección General de Impuesto Internos, en su Art. 4, literales C y D, los cuales disponen lo siguiente: "c) La transferencia de derechos de autor, propiedad industrial, permisos, licencias y otros derechos que no impliquen la transmisión de un mueble corporal; d) El arrendamiento de derechos o de bienes intangibles".

El precio pude estar sujetos a cambios debido a:

- **La variación en la tasa del dólar:** Muchos productos se importan o contienen componentes importados que están afectados por la tasa de cambio del dólar estadounidense. Si la tasa de cambio del dólar sube en relación con la moneda local, los productos importados pueden volverse más caros, lo que podría aumentar el precio final para los consumidores.
- **Políticas del fabricante sobre tiempos de renovación o adquisición del producto:** Los fabricantes pueden tener políticas que influyen en el precio final de un producto, como establecer precios según la demanda o introducir nuevas versiones o modelos que afectan la percepción del valor anterior. Además, los programas de renovación o adquisición pueden influir en el precio si incluyen descuentos, incentivos u otros términos que afecten el costo para el consumidor.

El costo estimado para la contratación de los servicios se hace en base a las informaciones disponibles en el SECP, en los catálogos de bienes y servicios y en el Sistema de Información de Precios, administrados por la Dirección General de Contrataciones Pública. Además, se tomó en cuenta las diferentes variables que pueden afectar el precio final de los mismos.

En cuanto a la determinación del tipo de contrato a celebrar, será un contrato de servicios y se espera llevar a cabo la firma de un contrato que contenga todos los elementos necesarios conforme a la normativa vigente, tales como: el objeto, detalle de los ítems, condiciones y tiempo de entrega, forma de pago, entre otros aspectos relevantes. La adjudicación será a favor de un único oferente y la vigencia del contrato será por el periodo de un (1) año.

Los criterios sociales, ambientales y económicos asociados a la contratación, con el propósito de generar los mayores beneficios posibles, con los recursos disponibles.

Por la naturaleza de los servicios que se pretenden renovar, se pudieran ponderar criterios sociales de inclusión para el desempate de las propuestas, en cuyo caso, se dará preferencia a aquellas ofertas donde el oferente haya demostrado la contratación de personas con discapacidad como una buena práctica de inclusión. Lo que debe evidenciarse con la certificación del CONADIS.

Regulaciones aplicables a los bienes, servicios u obras.

El Decreto 71-21 y la Comunicación MINPRE-DMI-2022 del 01/02/2022 establecen la necesidad de que la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) emita informes y peritajes técnicos para los bienes y servicios que se adquieran para las instituciones públicas en el marco de los procesos de compras y contrataciones relacionadas con Gobierno Digital.

Esto implica que la OGTIC tiene la responsabilidad de evaluar la idoneidad, eficiencia y seguridad de las soluciones tecnológicas que se pretenden adquirir para su uso en las instituciones públicas. Sus informes y peritajes técnicos ayudarán a garantizar que las adquisiciones cumplan con los estándares requeridos en materia de tecnología de la información y comunicación, así como con los objetivos de Gobierno Digital establecidos por el gobierno.

En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, a los catorce (14) días del mes de octubre del año dos mil veinticuatro (2024). ---

_____

Ly Mendez Vasquez
Departamento de Gestión de Seguridad de la Información