Informe de estudios previos
Para la adquisición del derecho de uso de herramienta de Gestión de Activos

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 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 **adquisición del derecho de uso de herramienta de Gestión de Activos,** 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).

- Opcionalmente, la solución también debe poder implementarse como (SaaS), desplegado en una instancia en la nube totalmente separada de los entornos de otros clientes.
- Si la instancia de nube se aprovisiona en una nube privada (como AWS, Azure o GCP), esta instancia debe poder alojarse en cualquiera de los entornos cercanos disponibles de la nube privada, y debe contar con copias de seguridad automáticas que permitan su restauración en caso de fallo.
- La solución debe contar con la opción de despliegue de nodos recopiladores adicionales que se conecten al nodo principal.
- Para obtener datos de redes parcialmente conectadas con conectividad limitada o reglas de firewall restrictas. O para agregar equilibrio de carga a la instalación.
- La solución debe contar con certificaciones SOC 2 Tipo 2 y SOC 3.
- El producto debe contar obligatoriamente con la certificación ISO 27001, acreditando la aplicación del marco para la estructura y gestión de la seguridad.
- Debe permitir la creación de roles de acceso y usuarios para acceder la plataforma.
- Debe permitir acceso local, a través de plataformas de autenticación LDAP y de single sign-on vía SAML. Sin costo adicional de licencias.
- Debe tener integración nativa con la base de datos de CISA (Known Vulnerabilities Database).
- La solución debe tener la opción de obtener detalles de vulnerabilidades de software de la base de datos nacional de vulnerabilidades (NVD) del NIST.
- Las credenciales para acceder a otras soluciones deben almacenarse de forma segura, localmente en la solución, o a través de la conexión con soluciones de gestión de secretos.
- Debe tener capacidad de tomar snapshots históricos de los datos para cualquier frecuencia calendario.
- Debe tener capacidad de poder monitorear la salud de la consola y sus colectores.
- Debe tener capacidad de definir calendarios de extracción globales o en forma individual para cada conector o API.
- Debe poder monitorear la salud de cada uno de los conectores y llevar un registro completo de los procesos de extracción de metadata.
- Debe tener capacidad de llevar pistas de auditoría de todas las acciones ejecutadas por usuarios de la plataforma.
- Debe tener capacidad de hacer extracciones de datos a demanda.
- La solución debe tener una API completa, accesible a través de clientes Restful y Phython, sin costos de licencia adicionales.

Inventario de Dispositivos

- Permite la consulta de un dispositivo, grupo o todos los dispositivos almacenados en el módulo de inventario de dispositivos.
- Permite hacer consultas de manera simple, donde se definen las condiciones basadas en los operadores de datos agregados en la plataforma o condiciones específicas para cada conector o API.
- Permite almacenar consultas y reutilizarlas como parte de condiciones dentro de otras consultas.
- Permite realizar consultas por diferentes criterios basados en la metadata extraída de cada conector o plataforma, como, por ejemplo, tipo de sistema operativo, versión del SO, Service packs aplicados, IP address, dominio, región y etc.

de seguridad deseada, la violación de la política de seguridad y cualquier otra cuestión relacionada con la gestión de activos.

- La solución debe tener, por defecto, un gráfico que permita enumerar la cantidad de dispositivos vistos por cada integración conectada, por separado para cada integración, ordenados de mayor a menor cantidad de dispositivos. Mostrando un número total y único de dispositivos después de la correlación.
- La solución debe tener, por defecto, un gráfico que permita enumerar la cantidad de usuarios vistos por cada integración conectada, por separado para cada integración, ordenados de mayor a menor cantidad de dispositivos. Mostrando un número total y único de usuarios después de la correlación.
- La solución debe contener modelos de dashboards predefinidas, incluidos paneles de visibilidad de activos, gestión de vulnerabilidades, descripción general del entorno de la nube, paneles que demuestren el cumplimiento y los riesgos y que puedan brindar visibilidad a la fuerza laboral remota.
- Los dashboards deben admitir actualizaciones dinámicas, permitiendo actualizaciones dinámicas basadas en criterios de filtro disponibles. De esta manera, es posible crear paneles genéricos, que se pueden filtrar en tiempo real para reflejar datos, por ejemplo, solo de una región o tipo de activo.
- Los dashboards deberían permitir comparar los resultados de las consultas de hoy con una fecha anterior.
- Debe tener la capacidad de generar informes ejecutivos predefinidos en formato PDF, archivos CSV o ambos.
- Los informes creados deben incluir gráficos creados en los paneles de la solución, una lista seleccionada de consultas guardadas para dispositivos o usuarios, o una combinación de paneles y consultas guardadas de una lista seleccionable.
- Debe permitir el envío automático de informes por correo electrónico, permitiendo la programación de estos envíos.
- Debe permitir la programación de informes para diferentes frecuencias de ejecución.

Automación de Acciones

- La solución debe tener la capacidad de imponer la ejecución de acciones en función de una consulta guardada, que puede realizar automáticamente una o más acciones en entidades que coincidan con los parámetros de la consulta (brechas de políticas).
- Las acciones de cumplimiento deben brindar la capacidad de mitigar, notificar y/o crear incidentes sobre las brechas identificadas.
- La solución debe admitir el enriquecimiento de datos para dispositivos y datos de usuario con información de fuentes de datos de terceros como Shodan, Censys, HaveIBeenPwned, Portnox y más.
- La solución también debe facilitar la adición o actualización de datos de dispositivos en una base de datos de gestión de configuración (CMDB).
- Permite la creación de trabajos ejecutando acciones como:
    - Poner etiqueta a diferentes activos.
    - Crear tiquetes en forma automática en diferentes ITSMs, incluidos Jira y Service Now.
    - Empujar datos desde la plataforma de inventario hacia otras tecnologías.
    - Actualizar los activos en la cobertura de gestión de vulnerabilidades, incluido como mínimo el soporte para Qualys, Tenable y Rapid7

Condiciones de pago

- Los pagos se harán previo presentoción de factura con Comprobante Gubernamental. En cada factura podrán ser solicitadas Certificaciones de la DGII y TSS o los fines de gestionar el pago.
- El pago se realizará dentro de los treinta (30) días laborales siguientes a la fecha de vencimiento de la factura que deberá ser emitida uno vez sean recibidos conforme los bienes y servicios solicitados.
- Lo empresa adjudicaría deberá mantenerse en todo momento al día con sus obligaciones fiscales y de seguridad social, paro poder recibir los pagos correspondientes o los servicios ofrecidos. En ese sentido, si por el no cumplimiento de estas obligaciones por porte del adjudicatario la Tesorería se ve imposibilitado de recibir los servicios objeto de la presente contratación, el contrato podrá ser rescindido dando pie a la adjudicación de la empresa que haya quedado en segundo lugar o a un nuevo proceso.
- Los pagos se harán por transferencia bancaria o lo cuento que el proveedor tenga registrada en DIGECOG, por lo que para recibir los pagos el suplidor debe encontrarse registrado como beneficiario en lo Dirección General de Contrataciones Publicas y tener cuenta registrada.
- La Tesorería de lo Seguridad Social realiza retención del Impuesto Sobre lo Renta de acuerdo con los Normas Legales Vigentes de lo Dirección General de Impuestos Internos.
- Lo empresa adjudicataria deberá entregar una certificación en la que establezca las fechas de inicio y fin de soporte y/o vigencia de las partes entregadas.

Unidad coordinadora del contrato

Por parte de la entidad contratante, la unidad coordinadora y ejecutora será la Dirección de Normas, Cumplimiento y Ciberseguridad, bajo la responsabilidad de **José Alberto Luna Peña,** asesor.

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 **del derecho de uso de herramienta de Gestión de Activos** es **RD$4,100.000.00,** en cuya virtud, de conformidad con el umbral establecido mediante la Resolución No. PNP-01-2024 emitida por la Dirección General de Contrataciones Públicas (DGCP), la forma idónea para satisfacer la necesidad es mediante un proceso de compra por montos debajo del umbral o compra directa, de conformidad con el artículo 45 del Reglamento de aplicación de la Ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios y Obras, aprobado mediante Decreto No. 416-23, el cual se caracteriza por ser un procedimiento simple y ágil, al tiempo que se garantiza la transparencia y eficiencia, en cumplimiento de los procedimientos establecidos.

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:

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). ---

José Alberto Luna Peña
Asesor Dirección de Normas, Cumplimiento y Ciberseguridad