INFORME DE ESTUDIOS PREVIOS
PARA LA ADQUISICION DE SERVICIO DE HERRAMIENTA DE GESTION DE ACTIVOS.

A fin de preparar los procedimientos de compras y contrataciones con la información precisa y suficiente que justifique la necesidad de la contratación y la modalidad de selección del contratista, es necesario que todo procedimiento de contratación se encuentre 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, por lo que la Tesorería de la Seguridad Social (TSS), como parte de la etapa precontractual ha procurado realizar el presente informe de estudios previos con la finalidad garantizar la correcta selección de los procesos, un mejor aprovechamiento de los recursos y una mayor eficiencia en la ejecución de los contratos.

El objetivo del presente informe es presentar los resultados de los estudios previos realizados por la **Dirección de Gestión de Riesgos, Cumplimiento y Ciberseguridad** para la **Adquisición de Servicio de Herramienta de Gestión de Activos,** en cumplimiento con los establecido en el Reglamento de aplicación de la Ley 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, aprobado mediante el Decreto NO. 416-23.

Objeto de la Contratación:

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 registro, recaudo, distribución y pago de las cotizaciones del Sistema Dominicano de Seguridad Social (SDSS), así como del Sistema Único de Información y Recaudo (SUIR). Es por esto que la Tesorería de la Seguridad Social (TSS) en su Plan Anual de Compras y Contrataciones (PACC), ha consignado para el año 2025, la **Adquisición de Servicio de Herramienta de Gestión de Activos,** con el fin de fortalecer la postura de seguridad de la institución mediante una capacitación avanzada, continua y personalizada. Este servicio permitirá a la institución gestionar la superficie de ataque de sus activos, tanto internos como externos. A su vez, brindará a la Dirección de Gestión de Normas, Cumplimiento y Ciberseguridad la capacidad de superar los desafíos de visibilidad y exposición mediante integraciones API con las herramientas existentes. Facilitará la consulta de datos consolidados, la identificación del alcance de las vulnerabilidades y de las brechas en los controles de seguridad, así como la oportuna resolución de los hallazgos.

Para llevar a cabo la contratación, el Decreto núm. 71-21 y la Comunicación MINPRE-DMI-2022 del uno (1) de febrero del año dos mil veintidós (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 el Gobierno Digital.

Especificaciones técnicas

Para la **Adquisición de Servicio de Herramienta de Gestión de Activos** se requiere que el servicio contenga las siguientes especificaciones técnicas:

Ítem	Rubro	Descripción	Cantidad	Unidad de medida	Especificaciones
1	81112501	**Adquisición de Servicio de Herramienta Gestión de Activos**	1	Licencia	*Ver especificaciones debajo.

- El licenciamiento debe ser basado en activos de duplicados y vigentes, bajo las modalidades de suscripción.
- La solución no debe requerir el uso de agentes
- El descubrimiento de activos y usuarios debe ser basado en una arquitectura de conectividad directa a otras plataformas tecnológicas, a través de API u otros protocolos (transferencia de archivos, servicios web, conexión directa, protocolo propietario etc.), sin depender de scanner o sensores proprios.
- La solución debe agregar, normalizar, de duplicar y correlacionar datos de más de 700 soluciones tecnológicas para ofrecer un inventario completo de dispositivos, activos en la nube, cuentas e identidades de usuario y etc.
- Debe poder implementarse localmente (on premise) a través de appliance virtual.
- La solución debe soportar su instalación como un appliance virtual, soportando al menos, VMware ESXi, Microsoft HyperV, Amazon AWS, Microsoft Azure o Google Cloud Platform (GCP).
- 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.
- Permite utilización de tags en las consultas, para fácil categorización.
- Permite la correlación de eventos entre diferentes adaptadores a fin de brindar mayor robustez a la plataforma.
- Permite el almacenamiento público y privado de consultas. Las consultas privadas son de acceso único del creador de estas.
- Permite utilizar filtros para cualquier condición desplegada en la metadata de los activos.
- Permite exportar a formatos PDF o CSV los resultados de una consulta.
- Cada activo debe tener su propio perfil, donde es posible ver todos los datos consolidados y correlacionados de otras soluciones, y es posible ver los datos en conjunto. O específico para cada solución.
- Solución debe admitir campos complejos que puedan mostrar una serie de parámetros. Por ejemplo, el campo Software instalado puede contener el campo Versión del software, el campo Nombre del software, el campo Proveedor del software, etc.
- Además del software, estos campos complejos deben admitir al menos hardware conectado, reglas de firewall, versiones de agentes, etc.
- La solución debe tener la opción que permita la creación de consultas, que ayuden a comprender cómo los activos se adhieren a las políticas.
- La solución debe tener la capacidad de definir una amplia variedad de filtros, desde los cuales puede profundizar hasta los activos que coinciden con los criterios de búsqueda. Por ejemplo: muestre solo los activos Windows que se hayan visto en los últimos 7 días.

Inventario de Usuarios

- La solución debe poder descubrir las entidades de usuario que son las identidades utilizadas para la autenticación y la propiedad de los dispositivos.
- La solución debe poder obtener información del usuario y correlacionarla desde diferentes adaptadores que contienen información de identidad como Microsoft Active Directory, Google Mobile Management (G-Suite), Okta y otros.
- La solución debe tener la capacidad de conectarse a Microsoft Azure Active Directory, con la posibilidad de visibilidad de las cuentas no utilizadas en Office 365.
- Debe permitir identificar propiedades específicas de usuarios de los directorios a que pertenecen.
- La solución debe tener la capacidad de generar consultas que permitan buscar cuentas cuya contraseña caducará, dentro de un período de tiempo específico.
- La solución debe tener la opción que permita la creación de consultas, que ayuden a comprender cómo los usuarios se adhieren a las políticas.
- La solución debe tener la capacidad de definir una amplia variedad de filtros, desde los cuales puede profundizar hasta los usuarios que coinciden con los criterios de búsqueda. Por ejemplo: muestre solo los usuarios que se hayan autenticado al dominio en los últimos 60 días.

Reportes

- La solución debe tener la posibilidad de crear dashboards que puedan presentar una vista inmediata basada en consultas existentes guardadas.
- Estos dashboards deben proporcionar un área única, consolidada y central para monitorear y absorber la visibilidad de todos los activos (dispositivos, usuarios, vulnerabilidades) en función de consultas guardadas, diseñadas para aclarar la política 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
- Aislamiento y des aislamiento de activos con plataformas EDR, incluida la compatibilidad con Crowstrike, SentinelOne, Palo Alto Networks Cortex XDR y Microsoft Defender (ATP), como mínimo.
- Gestión de activos en todos los servicios de autenticación, lo que le permite habilitar o deshabilitar activos, incluida la compatibilidad con Microsoft Active Directory, Microsoft Azure AD y Okta, como mínimo.
- Debe admitir el etiquetado de instancias en la nube y, como mínimo, admitir Microsoft Azure, Amazon AWS y Google Cloud Platform (GCP).
- Debe admitir la adición de activos a una collection de Microsoft System Center Configuration Manager (SSCM)
- Gestión de usuarios y grupos que permite habilitar o deshabilitar usuarios, incluido el soporte para Microsoft Active Directory, Gsuite y Okta como mínimo.

Los productos requeridos serán validados bajo visita de parte del personal autorizado por la Tesorería de la Seguridad Social (TSS) que permita la comprobación de los requisitos establecidos en las especificaciones técnicas indicadas.

Análisis de oferta y costo estimado

En virtud de las investigaciones realizadas, se ha podido identificar que en el mercado existen varios proveedores que pueden ofrecer el servicio en el territorio de la República Dominicana, por lo que, luego de consultar los costos en el mercado nacional, así como los precios

publicados en el Sistema de Información de Precio, administrado por la Dirección General de Contrataciones Públicas, se determinó que el costo estimado de la contratación es de **CUATRO MILLONES CIEN MIL PESOS DOMINICANOS CON 00/100** (**RD$4,100.000.00).**

Plazo y Lugar de Trabajo

La contratación será realizada bajo el periodo de **1 año** y el lugar de ejecución de los servicios será en el domicilio de la Tesorería de la Seguridad Social (TSS), ubicado en la Avenida Tiradentes No. 33, Torre de la Seguridad Social, Quinto Piso, Ensanche Naco, Santo Domingo, Distrito Nacional.

Modalidad de procedimiento aplicable

Conforme el costo estimado de la contratación se ha determinado tomando en cuenta la Resolución Núm. PNP-01-2025 que establece los umbrales topes para la determinación de la modalidad de selección de los procedimientos de contratación pública, correspondientes al año dos mil veinticinco (2025) y la naturaleza de lo requerido, que la modalidad de la contratación será a través de un procedimiento de **comparación de precios.**

Tipo de contrato

El contrato a suscribir será un contrato de **servicios** por el periodo de **1 año,** el cual deberá ser suscrito en la fecha que establezca el cronograma de actividades del pliego de condiciones que será elaborado, y en un plazo no mayor a veinte (20) días hábiles, contados desde la fecha de notificación de la adjudicación, de conformidad con el artículo 164 del Reglamento núm. 416-23.

Supervisor del contrato

La Tesorería de la Seguridad Social ha designado como supervisor o responsable del contrato a la Dirección de Normas, Cumplimiento y Ciberseguridad, bajo la responsabilidad de **José Alberto Luna Peña,** asesor de la Dirección de Normas, Cumplimiento y Ciberseguridad.

Condiciones de pago

El pago será realizado en un **único pago** conforme se indica a continuación:

El adjudicado deberá emitir una factura con Comprobante Fiscal Gubernamental que será pagado dentro de los treinta (30) días laborables siguientes a la fecha de vencimiento de la factura, luego del recibido conforme de los servicios por la Dirección de Normas, Cumplimiento y Ciberseguridad.

Al recibir cada factura podrá ser solicitado certificaciones de la DGII y la TSS a los fines de gestionar el pago, por eso el adjudicado deberá mantenerse al día en sus obligaciones fiscales y de Seguridad Social para recibir los pagos correspondientes.

Los pagos se harán por transferencia bancaria a la cuenta que el proveedor adjudicado tenga registrada en la DGCP, por lo que para recibir los pagos el proveedor adjudicado debe encontrarse como beneficiario en la Dirección General de Contrataciones Públicas y debe tener cuenta registrada en pesos dominicanos.

La Tesorería de la Seguridad Social realizar retención de los impuestos que corresponda de acuerdo con las normas legales vigentes de la Dirección General de Impuestos Internos.

En caso de resultar adjudicada una MIPYME, en virtud de lo establecido en el Artículo 155 del Reglamento de Aplicación de la Ley núm. 340-06 aprobado mediante Decreto núm. 416-23, la entidad contratante procederá a realizar un primer pago por concepto de anticipo correspondiente al 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, contra presentación de una Póliza de Seguro o Garantía Bancaria que cubra la totalidad del Avance Inicial, y de la factura de tipo anticipo con número de comprobante fiscal gubernamental.

La suma restante correspondiente al ochenta por ciento (80%) del monto adjudicado será pagada en un único pago luego de del recibido conforme de los servicios por la Dirección de Normas, Cumplimiento y Ciberseguridad en un plazo no mayor a treinta (30) días hábiles. En ningún caso, está permitido que el proveedor reciba el pago total del servicio sin que el objeto del contrato se haya cumplido.

Garantías requeridas para el procedimiento de selección

Con la finalidad de garantizar que los oferentes y eventuales adjudicatarios no retiren sin causa justificada las ofertas presentadas en el procedimiento de selección, los oferentes/proponentes deberán constituir una **garantía de seriedad de su oferta** por un monto equivalente a uno por ciento (1%) del monto de la oferta a presentar.

Asimismo, para poder suscribir el contrato el o los adjudicatarios deberán constituir previamente una **garantía de fiel cumplimiento** de contrato en favor de la Tesorería de la Seguridad Social, para asegurar que cumplirá con las condiciones y cláusulas que serán establecidas en el pliego de condiciones y en el contrato que se derive de este. Esta garantía será equivalente al cuatro por ciento (4%) del monto adjudicado y en caso del adjudicado ser MIPYME, el equivalente será uno por ciento (1%) del monto adjudicado.

En la ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, a los Quince (15) días del mes de octubre del año dos mil veinticinco (2025). ---

_____

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