Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

INF-0420/25

INFORME SOLICITUD DE ASISTENCIA

TESORERÍA DE LA SEGURIDAD SOCIAL

TSS

MAYO 22, 2025.-

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Informe

Luego de un cordial saludo, sirva la presente para exponer consideraciones de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), respecto al proceso de compra para la **adquisición derecho a uso herramienta de gestión de activos,** el cual se nos ha presentado como dirección ejecutiva del gabinete de innovación y desarrollo digital.

Observaciones:

- Se adjunta carta de solicitud
- Se adjunta justificación de compra
- Se adjunta pliego de condiciones

A groso modo se solicita:

- 1 Derecho de Uso Herramientas de Gestión Activos.
    - 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).

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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).

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- 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, HavelBeenPwned, 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)

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Gestión de usuarios y grupos que permite habilitar o deshabilitar usuarios, incluido el soporte para Microsoft Active Directory, Gsuite y Okta como mínimo.

Conclusión:

Luego de revisar la documentación aportada, verificar la solicitud y sus soportes, evaluamos las especificaciones técnicas y consideramos que cumplen con todos los aspectos necesarios requeridos y no solapan ningún proyecto que haya de ejecutarse desde la Agenda Digital 2030, esta aprobación tiene vigencia hasta el 20 de agosto 2025.

Mario Adames
Encargado Departamento Asistencia Técnica Especializada
Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)