

FICHA TÉCNICA

OBJETO: RENOVACIÓN DE LA SUSCRIPCIÓN DE LA SOLUCIÓN INTEGRAL DE GESTIÓN DE CIBEREXPOSICIÓN Y DATOS FILTRADOS.

ESPECIFICACIÓN DEL OBJETO		
Denominación Técnica:		Ciber exposición y Servicio de Exposición de Datos Filtrados, seguridad y gestión de vulnerabilidades
Código UNSPSC		43222500 - Equipo de seguridad de red 43233200 - Software de seguridad y protección 81111800 - Servicios de Sistemas y Administración de componentes de sistemas 81112000 - Servicios de datos 81112200 - Mantenimiento y soporte de software
ÍTEM	CARACTERÍSTICA	MINIMO REQUERIDO
1.	Módulos de licencias a renovarse	El Instituto de Desarrollo Urbano - IDU requiere renovar la suscripción de la solución integral de Gestión de Ciberexposición y datos filtrados (plataforma Tenable One) con la que actualmente cuenta la Entidad, por un periodo de 12 meses contados a partir de su activación.
		A continuación, se relaciona el requerimiento solicitado, incluyendo su descripción técnica conforme a la plataforma Tenable One con la que actualmente cuenta la entidad y su respectivo alcance, el cual se detalla en el presente documento:

2. Requisitos Técnicos Mínimos de la Plataforma

La plataforma debe garantizar la continuidad operativa manteniendo o superando las siguientes capacidades técnicas unificadas con las que actualmente cuenta el IDU:

- **Gestión Centralizada:** Plataforma única de gestión de exposición cibernética, que integre en un solo inventario los hallazgos de vulnerabilidades de Activos TI, recursos cloud, contenedores, aplicaciones web y sistemas de identidad, con motor de análisis basado en grafos y visualización de rutas de ataque mediante el framework MITRE ATT&CK, identificación de activos críticos, debe mantener un inventario único y deduplicado de activos con actualización automática para los recursos cloud, etiquetado de activos de forma manual y dinámica, gestión de acceso por basado en roles (RBAC), y capacidad de integración via API.
- **Escaneo de Vulnerabilidades (2.200 activos):** Escaneo de los activos TI de la entidad, priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación, capacidad de simular ejercicios de explotación benignos para confirmar la presencia de vulnerabilidades, soporte de reglas YARA para la identificación de malware, y un API que permita integraciones programáticas.
- **Escaneo de Aplicaciones Web (100 FQDN):** Visibilizar todas las vulnerabilidades sobre los sitios web y aplicaciones basadas en Rest, escaneo de aplicaciones desarrolladas en

FICHA TÉCNICA

OBJETO: RENOVACIÓN DE LA SUSCRIPCIÓN DE LA SOLUCIÓN INTEGRAL DE GESTIÓN DE CIBEREXPOSICIÓN Y DATOS FILTRADOS.

frameworks JavaScript, AJAX, HTML5 y Single Page Applications, clasificación en OWASP Top 10, detección de problemas mediante SSL/TLS Scan y Config Audit Scan, autenticación avanzada, incluyendo form-based authentication, cookie-based authentication, NTLM support y Selenium-based authentication. Debe soportar integraciones vía API documentadas.

- **Seguridad Superficie de Ataque Externa (120 activos):** Identificación de activos conocidos y desconocidos, con base en registros DNS, direcciones IP y ASN, categorización con modelo de datos enriquecido de más de 200 campos de metadatos, monitorear y notificar los cambios sobre los activos expuestos a internet de manera diaria o semanal, descubrir dominios relacionados a los activos identificados suministrando razones de su vinculación, y generar capturas de pantalla de los sitios que dispongan de un portal web.
- **Seguridad en la Nube Pública (50 activos):** CNAPP nativamente unificada y deberá integrar, como mínimo, las siguientes capacidades en una única consola y bajo un modelo de datos correlacionado: CSPM, CWPP, CIEM y Seguridad de Infraestructura como Código (IaC), capacidad de correlacionar hallazgos entre estos distintos módulos para identificar y priorizar rutas de ataque complejas en el entorno de nube, y generación de recomendaciones granulares de en lenguajes nativo de la nube, como JSON o Terraform.
- **Seguridad en Directorio Activo (2.000 usuarios):** Monitoreo continuo sin instalación de agentes, ni activaciones de funcionalidades, ni la creación de cuentas con privilegios. Análisis basado en grafos, capacidad de auditoría con detección de malas prácticas, alertar de forma automática ataques dirigidos como Golden Ticket, Password Spraying, DCSync, DCShadow, OS Credential Dumping, PetitPotam, Kerberoasting y extracción de NTDS, a partir de una cuenta sin privilegios, y debe soportar una cuenta señuelo cuyo único propósito sea detectar a un atacante que intente comprometer la red a través del directorio activo.
- **Gestión de Actualizaciones (2.000 activos):** Optimización del ancho de banda de la red mediante peer to peer para distribución de parches, admitiendo la entrega fuera de la red para garantizar la entrega sin importar su estado de conexión, con sistema de aprobación por grupos y responsabilidades, implementación por fases y de forma automatizada, basada en agentes que permitan la distribución instantánea de políticas, y con consola independiente de la de vulnerabilidades, sin embargo con capacidad de intercambio de información de riesgos y probabilidades de explotación de brechas.

3. Condiciones del Servicio y Soporte

3.1. Generalidades

- **Tiempo de Cobertura:** Doce (12) meses contados a partir de su activación.
- **Lugar del Servicio:** Sede principal IDU (Bogotá D.C., Calle 22 N° 6 – 27 Piso 4) o según requerimiento.
- **Certificaciones de Fábrica:**
- El oferente debe presentar certificado de Partner o distribuidor directo autorizado del fabricante (Tenable) con nivel de membresía Silver o Superior.
- El oferente debe aportar una certificación no mayor a 90 días calendario de expedición a nombre de la entidad donde se indique de parte del fabricante el periodo de suscripción del licenciamiento, las cantidades y tecnologías ofertadas para la renovación.

3.2. Esquema de Soporte Técnico

- **Mesa de Servicios:** Soporte 7x24 para atención de incidentes (por el fabricante o canal autorizado) y soporte 5x8 con personal dedicado remoto para gestión de casos,

FICHA TÉCNICA

OBJETO: RENOVACIÓN DE LA SUSCRIPCIÓN DE LA SOLUCIÓN INTEGRAL DE GESTIÓN DE CIBEREXPOSICIÓN Y DATOS FILTRADOS.

acompañamiento, afinamiento de la herramienta y orientación en la remediación.

- **Acompañamiento:** El proveedor no asume administración ni operación de infraestructura del IDU, pero debe realizar recomendaciones y pautas de remediación claras.

3.3. Entregables Requeridos

- Carta o soporte de acceso a la suscripción a nombre del IDU por un (1) año.
- Informes de tres (3) evaluaciones (assessments) durante la vigencia de la suscripción, una cada cuatro (4) meses, en promedio, a fin de ajustar parámetros y configuraciones de la plataforma.
- Transferencia de conocimiento (20 horas) enfocadas en administración y operación de cada una de las herramientas que componen la solución, para al menos 2 personas designadas por la Entidad a través del supervisor.

4. Niveles de servicio (ANS) de disponibilidad de la solución

Categoría	Tiempo de Respuesta Inicial	Tiempo Máx. Solución o Escalamiento	Responsable
Crítico (P1)	≤ 30 minutos	≤ 4 horas o escalamiento inmediato a fabricante	Soporte Nivel 1 / 2
Alta (P2)	≤ 1 hora	≤ 8 horas hábiles	Soporte Nivel 1 / 2
Media (P3)	≤ 4 horas	≤ 24 horas hábiles	Soporte Nivel 1
Baja (P4)	≤ 8 horas hábiles	≤ 48 horas hábiles o según agenda	Soporte Nivel 2 / Coordinador

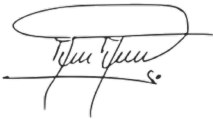
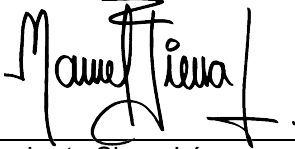
5. Perfil del Equipo de Trabajo

Rol	Formación Académica	Experiencia Requerida
Gerente del Proyecto	Título profesional en Ingeniería de Sistemas / Ingeniería electrónica / Ingeniería de Software / Ingeniería de Telecomunicaciones según NBC del SNIES. Especialización/Posgrado en Gerencia de Proyectos, Seguridad de la Información o afines.	General: 8 años desde la expedición de matrícula. Específica: 4 años en roles de liderazgo o gerencia en proyectos de ciberseguridad o seguridad de la información.

FICHA TÉCNICA

OBJETO: RENOVACIÓN DE LA SUSCRIPCIÓN DE LA SOLUCIÓN INTEGRAL DE GESTIÓN DE CIBEREXPOSICIÓN Y DATOS FILTRADOS.

Ingeniero de servicios y soporte	Título profesional en Ingeniería de Sistemas, o Ingeniería de Sistemas Informáticos, o Ingeniería electrónica, o Ingeniería de Telecomunicaciones. Deberá contar con título de posgrado según núcleo básico de conocimiento de acuerdo (NBC) SINES Informática o Ciberseguridad. Certificación técnica vigente emitida por el fabricante TENABLE.	General: 3 años en el sector TI contados a partir de la obtención de la tarjeta profesional Específica: 3 años en cargos relacionados con análisis de seguridad de la información
---	--	---

Elaborado por	Aprobado por
Firma: 	Firma: 
Nombre: Ángel Antonio Díaz Vega	Nombre: Manuel Humberto Sierra López
Cargo o vinculación: Contratista STRT	Cargo o vinculación: Subdirector Técnico de Recursos Tecnológicos