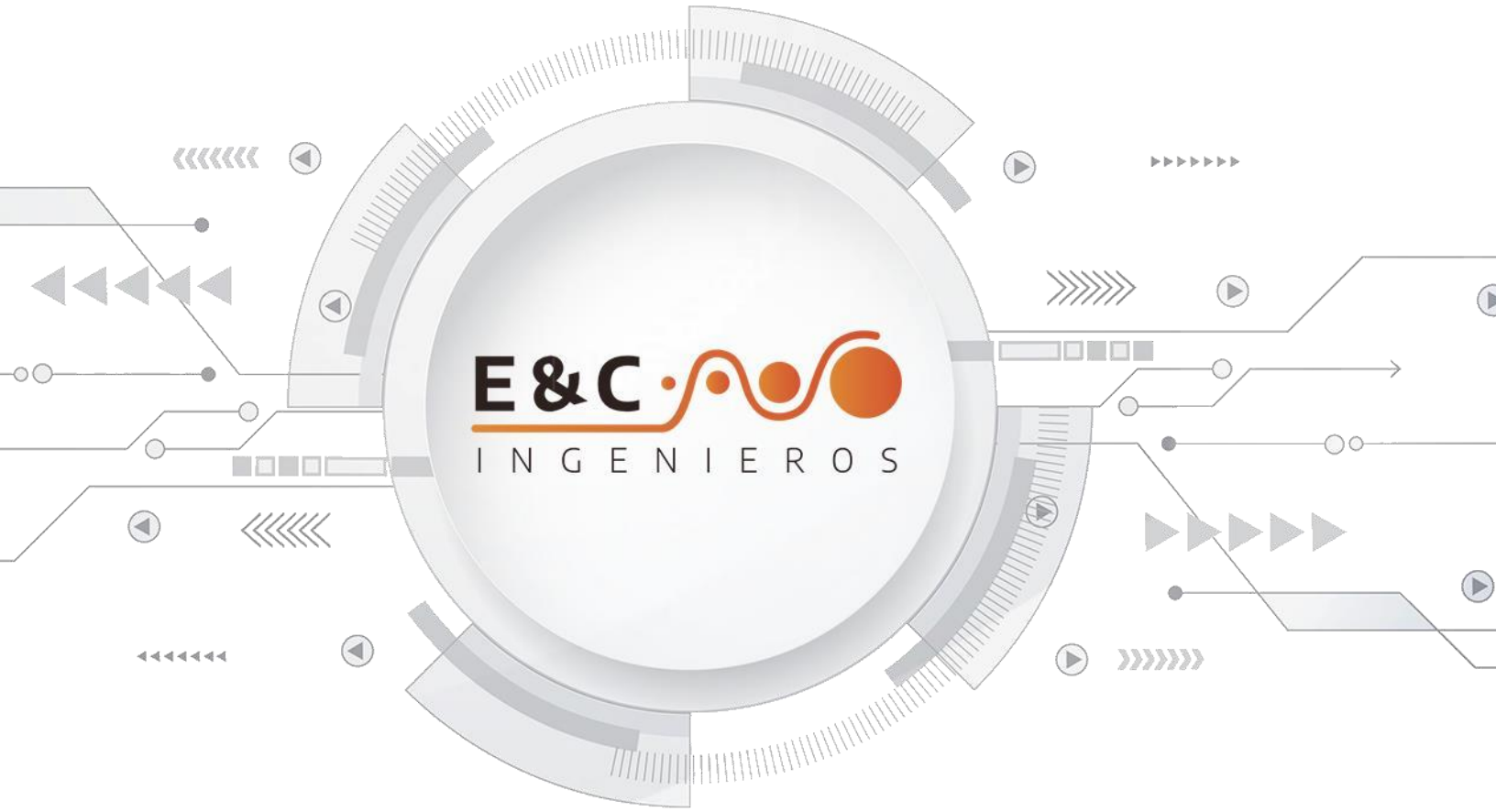
E&C INGENIEROS



PROPUESTA COMERCIAL

DIMAR.

02 de marzo de 2026

www.eycingenieros.com
comercial@eycingenieros.com
(601) 4 824681
Carrera 74 A # 52 A - 70

DOCUMENTO CONFIDENCIAL

El presente documento ha sido preparado para la presentación de nuestros servicios en esta propuesta. Los servicios y productos indicados en el presente documento han sido diseñados exclusivamente para ser prestados a DIMAR.*, a partir de la fecha mostrada en la carátula de este documento queda sin efecto cualquier documento anterior o acuerdo verbal relacionado con los servicios o productos aquí indicados. La información contenida en este documento no debe divulgarse fuera del* DIMAR. *y no debe ser duplicada, usada o divulgada completamente o en parte con propósitos distintos a su evaluación. Este documento, incluyendo cualquier anexo y apéndice, contiene información, contenido y estructura que constituyen secretos de marca y/o información financiera o comercial de carácter confidencial de EYC INGENIEROS, catalogado como propiedad intelectual. Esta información es entregada a* DIMAR. *En el entendimiento de que no será utilizada para otros fines que no sean la evaluación y control de esta propuesta.*

¿QUIÉNES SOMOS?

Con más de 20 años de experiencia en EYC INGENIEROS trabajamos día a día por la satisfacción de nuestros clientes.

Por medio del trabajo en equipo aprendemos y nos adaptamos para ser cada vez mejores, a la vez que mejoramos y diseñamos continuamente nuestros procesos ajustándonos a la medida de nuestros clientes, para asegurar así un crecimiento mutuo.

Nos apalancamos en un recurso humano capacitado, competente, comprometido y utilizamos las mejores herramientas tecnológicas parar generar estrategias organizacionales que hagan de las relaciones con nuestros clientes internos y externos una experiencia única.



www.eycingenieros.com
comercial@eycingenieros.com
(601) 4 824681
Carrera 74 A # 52 A - 70

E&C INGENIEROS

NUESTRAS CERTIFICACIONES

SC-CER573307

- Enfoque en el cliente
- Mejora continua
- Procesos eficaces
- Capacitación y desarrollo del personal

- Cumplimiento de la Legislación
- Mejora en el Desempeño
- Gestión de Impactos
- Capacitación del Personal

SA-CER837189

ISO 20000
LL-C (Certification)
No. 573628

- Servicio y SLA
- Disponibilidad
- Gestión de capacidad
- Soporte técnico

- Confidencialidad
- Integridad
- Disponibilidad
- Gestión de riesgos

ISO 27001
LL-C (Certification)
No. 573628

www.eycingenieros.com
comercial@eycingenieros.com
(601) 4 824681
Carrera 74 A # 52 A - 70

E&C INGENIEROS

NUESTROS CASOS DE ÉXITO

Abarcamos más de **200** proyectos en entidades gubernamentales y 200 empresas privadas que cuentan con nuestros servicios,

200



www.eycingenieros.com
comercial@eycingenieros.com
(601) 4 824681
Carrera 74 A # 52 A - 70

E&C INGENIEROS

NUESTRAS LÍNEAS DE SERVICIO



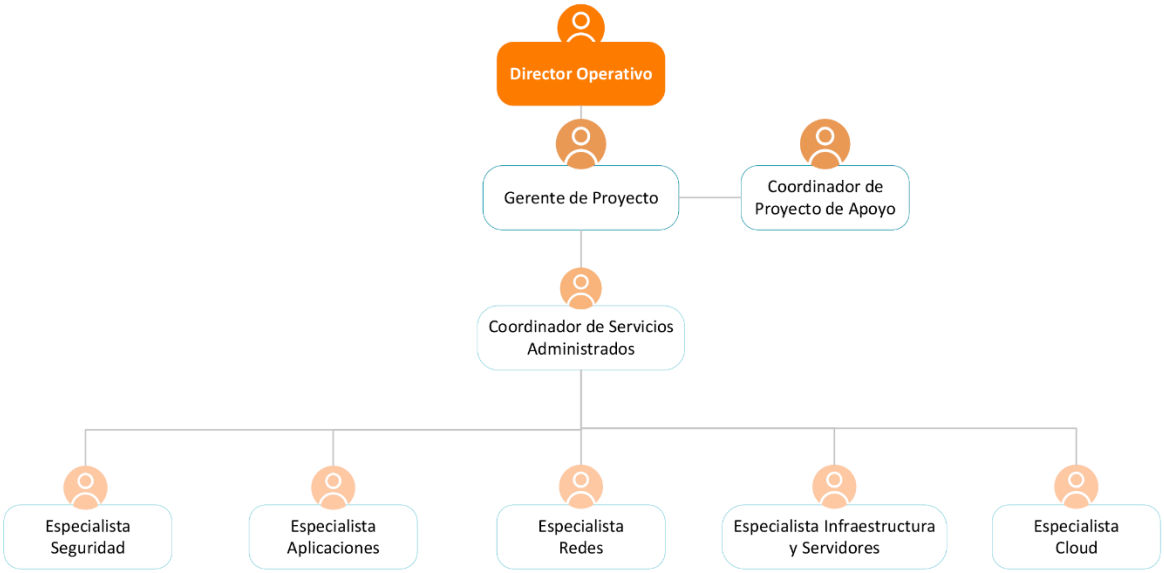
- SECURITY OPERATION CENTER
- CONSULTORÍA SEGURIDAD DE LA INFORMACIÓN
- SEGURIDAD PERIMETRAL
- PENTESTING / ETHICAL HACKING

- NOC — NETWORK OPERATION CENTER
- BOC — BACKUP OPERATION CENTER
- ATI — ADMINISTRACIÓN DE TI
- CTI — CONSULTORÍA TI
- NWK — NETWORKING

- CORREO ELECTRÓNICO CERTIFICADO
- SEDE DIGITAL
- FIRMAS DIGITALES
- ESTAMPA DE TIEMPO

www.eycingenieros.com
comercial@eycingenieros.com
(601) 4 824681
Carrera 74 A # 52 A - 70

MODELO DE OPERACIÓN



Modelo de operación para el área de Especialistas en Servicios Administrados (SAD)

Bogotá D.C., 02 de marzo 2026

Señores:
DIMAR.
Bogotá

REF. Licencia Monitoreo TENABLE IO para 200 activos (VM)

En EYC Ingenieros S.A.S. es de nuestro agrado presentar la siguiente propuesta, orientada a fortalecer la eficiencia y control operativo de su organización, es por esto que la misma cumple con todos y cada uno de los requerimientos establecidos en el documento denominado.

ALCANCE

Requerimientos
Generales • La solución debe integrar completamente el escaneo de vulnerabilidades y la evaluación de la configuración dentro de un solo licenciamiento permitiendo también la consolidación de datos, análisis y consultas para estos dos casos de uso. • La solución debe estar licenciada para realizar el escaneo sobre doscientos (200) activos de red por un periodo de doce (12) meses. • La solución debe incluir una capacidad integrada de exploración activa y pasiva para lograr una visibilidad más completa de las vulnerabilidades, considerando el análisis en tiempo real. • La solución debe incluir paneles gráficos personalizables que permitan ajustar la información presentada a las necesidades puntuales del usuario. • La solución debe ofrecer entrenamiento gratuito en línea como parte de la oferta. • La solución debe ofrecer soporte técnico 24/7/365.
Arquitectura • La solución debe proporcionar un modelo de almacenamiento integrado que no requiera el uso de bases de datos externas. • La solución debe proporcionar una API integral para la automatización de procesos y la integración con aplicaciones de terceros. • La solución debe incluir la opción de uso de agentes para aquellos dispositivos que no puedan ser analizados por otros medios de manera frecuente. • La solución debe ofrecer diferentes opciones de implementación, como máquina virtual soportada por el fabricante o como aplicación a instalar sobre un sistema operativo (para los módulos de análisis o colección de datos). • La solución debe ser capaz de analizar activos en las redes internas de los clientes, así como activos externos / disponibles públicamente. • La solución debe facilitar el uso de motores de análisis ubicados en la nube sin costo adicional y que permitan la recolección de datos sobre activos que se encuentren expuestos hacia internet. • La solución debe permitir la instalación de sensores en soluciones de nube pública como AWS o Azure. Dichos sensores deben encontrarse disponibles en los catálogos de cada uno de estos proveedores. • La solución debe estar en capacidad de integrarse con nubes públicas como Azure y AWS con el fin de detectar proactivamente la aparición de instancias nuevas para que se reflejen en el inventario de activos. • La solución debe estar en capacidad de integrarse con AWS con el fin de hacer un descubrimiento de vulnerabilidades a partir del uso de herramientas nativas de dicha nube, evitando la instalación de agentes o el uso de un scanner en la VPC (Virtual Private Cloud).
Control de acceso • La solución debe proporcionar control de acceso basado en roles (RBAC) para controlar el acceso del usuario a conjuntos de datos y funcionalidades específicas.

• La solución debe proporcionar la capacidad de restringir los permisos de flujo de trabajo para incluir, aceptar y volver a ejecutar clasificaciones de riesgo para vulnerabilidades. • La solución debe poder definir y administrar grupos de usuarios, incluida la limitación de las funciones de escaneo y el acceso a informes.
Exploración • La solución debe soportar diversas plataformas de motores de escaneo incluyendo Windows, Linux, Mac OS, así como máquinas virtuales. • Múltiples motores de recolección de información (escáner activo, pasivo o agente) deben permitirse sin que esto represente un costo adicional. • La solución debe admitir múltiples motores de escaneo distribuidos geográficamente y administrados por una consola central. • La solución debe ser configurable para limitar la carga sobre la red ocasionada por el escaneo para evitar la generación de tráfico que podría interrumpir la operación normal de la red. • La solución debe proporcionar la capacidad de admitir el escaneo sin conexión y la importación de resultados en la plataforma. • La solución debe permitir la entrada y el almacenamiento seguro de credenciales de usuario, incluidas las cuentas locales y de dominio de Windows, y Unix su y sudo. • La solución debe proporcionar la capacidad de escalar privilegios en los objetivos desde el acceso normal del usuario al acceso con roles de administración (root/ administrador). • La solución debe permitir la programación de escaneos personalizados, incluida la capacidad de ejecutar escaneos en momentos designados, con una frecuencia predeterminada. • La solución debe estar en capacidad de realizar búsquedas de datos confidenciales en los endpoint.
Descubrimiento de activos • La solución debe estar en capacidad de integrarse con varios sistemas de administración de dispositivos móviles (MDM) diferentes con el fin de extender la visibilidad y análisis de vulnerabilidades sobre dichos equipos. • La solución debe ser capaz de detectar servicios que se ejecutan en puertos no estándar. • La solución debe ser capaz de detectar servicios configurados para no mostrar pancartas de conexión. • La solución debe ser capaz de probar varias instancias del mismo servicio que se ejecuta en diferentes puertos. • La solución debe ser capaz de escanear hosts muertos (dispositivos que no responden al ping). • La solución debe admitir el uso opcional de netstat para una enumeración rápida y precisa de los puertos abiertos en un sistema cuando se proporcionan las credenciales. • La solución debe admitir el uso de SMB y WMI para escanear sistemas Windows. • La solución debe ser capaz de iniciar automáticamente los servicios de registro remoto en los sistemas Windows al realizar una exploración con credenciales, y luego detener automáticamente el servicio una vez que se complete la exploración. • El escáner debe admitir Secure Shell (SSH) con la capacidad de escalar privilegios para escaneos de vulnerabilidades y auditorías de configuración en sistemas basados en Unix. • La solución debe proporcionar la capacidad de ajustar las políticas de escaneo para un impacto mínimo en las redes y los objetivos. • El producto debe proporcionar un descubrimiento activo y pasivo de puntos de acceso inalámbrico (WAP).
Evaluación de vulnerabilidad • La solución debe ser capaz de realizar pruebas para la detección de vulnerabilidades locales y remotas sin la necesidad de un agente en el dispositivo de destino. La solución debe ser capaz de realizar pruebas de agentes para la detección de vulnerabilidad local sin costo adicional.

• La solución debe ser capaz de rastrear los cambios de DHCP al asociar los resultados de escaneo de un sistema dado con algo diferente a la dirección IP.

• La solución debe ser compatible con CVE y proporcionar al menos 10 años de cobertura de CVE.

• La solución debe proporcionar auditorías de parches para los sistemas operativos y aplicaciones de Microsoft para incluir Windows 7, Windows 2008, Internet Explorer, Microsoft Office, IIS, Exchange y más.

• La solución debe proporcionar auditorías de parches para todos los principales sistemas operativos Unix para incluir Mac OS, Linux, Solaris, IBM AIX, HP-UX y más.

• La solución debe proporcionar cobertura para aplicaciones de terceros como Java y Adobe.

• La solución debe proporcionar integración con los sistemas de administración de parches para la auditoría de parches y los informes delta contra los hallazgos de escaneo como Microsoft WSUS / SCCM, Redhat Satellite, IBM Tivoli Endpoint Manager y Symantec Altiris.

• La solución debe proporcionar integración con Mobile Device Managers (MDM) para el descubrimiento y la auditoría de dispositivos móviles.

• La solución debe incluir la calificación de vulnerabilidad de acuerdo con el estándar aceptado por la industria, es decir, el Sistema de calificación de vulnerabilidad común Versión 3 (CVSS 3).

• La solución debe proporcionar información acerca de la capacidad de explotación de la vulnerabilidad por parte de terceros como Core, Metasploit y Canvas.

• La solución debe proporcionar información de vulnerabilidades que pueden ser explotadas por malware.

• La solución debe seleccionar de forma inteligente las pruebas a realizar basándose en la información obtenida de los escaneos iniciales para intentar realizar pruebas adicionales basadas en la información obtenida previamente sobre un dispositivo o host dado.

• La solución debe permitir que las pruebas seleccionadas se habiliten o deshabiliten durante los escaneos programados.

• La solución no debe depender de la capacidad del sistema operativo para programar tareas.

• La solución debería admitir el escaneo IPv6, con descubrimiento pasivo de objetivos IPv6.

• Las soluciones deben rastrear con precisión los activos y sus vulnerabilidades, incluidos los activos de TI altamente dinámicos como dispositivos móviles, máquinas virtuales e instancias en la nube.

• La solución debe asignar un puntaje adicional a cada vulnerabilidad que refleje la probabilidad de que esta sea aprovechada por un atacante, teniendo en consideración atributos como la existencia de un exploit, si se han presentado víctimas de dicha vulnerabilidad, entre otros.

Auditoría de configuración

• La solución debe ser capaz de realizar auditorías de cumplimiento sin la necesidad de un agente instalado en el dispositivo de destino.

• La solución debe proporcionar puntos de referencia de auditoría de seguridad y configuración para estándares de cumplimiento normativo, así como otros estándares de mejores prácticas de la industria.

• La solución debe proporcionar puntos de referencia de auditoría de seguridad y configuración para las mejores prácticas del proveedor, como Microsoft, Linux, soluciones MDM como Airwatch, enrutadores y conmutadores, firewalls y VMware.

• La solución debe proporcionar una auditoría de los sistemas operativos de Microsoft a nivel de configuración.

La solución debe proporcionar una auditoría de los principales sistemas operativos Unix a nivel de configuración.

• La solución debe proporcionar una auditoría de las bases de datos a nivel de configuración.

• La solución debe proporcionar una auditoría de la infraestructura de red a nivel de configuración.

• La solución debe proporcionar una auditoría de la administración de dispositivos móviles a nivel de configuración.

• La solución debe proporcionar auditorías de paquetes antivirus específicos.

• La solución debe estar en capacidad de auditar la presencia de información de identificación personal (PII) y otro contenido confidencial. • La solución debe permitir que las políticas de auditoría sean personalizables para las necesidades específicas de la organización. • La solución debe proporcionar puntos de referencia para dar cumplimiento a las recomendaciones del CIS. • La solución debería ofrecer soporte SCAP.
Informes • La solución debe proporcionar la capacidad de automatizar la generación de informes. La solución debe estar en capacidad de producir informes ad hoc mientras se visualizan los resultados en la consola. • La solución debe admitir la capacidad de producir informes en pdf y pdf cifrado de manera programada o por demanda. • La solución debe proporcionar una biblioteca de plantillas para los páneles de presentación de datos. • La solución debe permitir la exportación de los tableros de datos presentados en formato Nessus, CSV, PDF y HTML.

OFERTA ECONÓMICA

ÍTEM	DESCRIPCIÓN TÉCNICA DE LOS BIENES Y/O SERVICIOS POR CONTRATAR	UNIDAD DE MEDIDA	CANTIDAD	VR UNITARIOS	IVA	TOTAL
1	Licencia Monitoreo TENABLE IO para 200 activos (VM)	Unidad	200	$ 300.756,89	N/A	$ 60.151.377,83

Cordialmente,

EYC INGENIEROS SAS
NIT: 900.024.202-1
ELQUIN LEONARDO PEREZ CRUZ
REPRESENTANTE LEGAL

CONDICIONES COMERCIALES

Precios y Validez

- Los precios indicados en esta propuesta están expresados en pesos colombianos y son válidos por un período de noventa (90) días desde la fecha de emisión de la propuesta.
- Cualquier cambio posterior en los precios será notificado con antelación y estará sujeto a negociación.

Formas de pago

- El pago debe realizarse mediante transferencia bancaria, en un plazo máximo de treinta (30) días después de la emisión de la factura.
- Se requiere un anticipo del 50% al momento de la aceptación de la propuesta, con el saldo pagadero según los términos acordados.

Plazos de entrega

- El plazo de entrega comenzará a contar una vez recibido el anticipo y confirmada la aceptación de los términos y condiciones por ambas partes.
- Las fechas de entrega son estimadas y pueden estar sujetas a ajustes en función de factores externos.

Garantías

- Una vez aprobada la propuesta, el cliente asume la responsabilidad de gestionar la adquisición de los equipos necesarios y, en caso de devolución, cubrir cualquier penalización aplicable

Política de cancelación

- Cualquier cancelación deberá ser notificada por escrito con al menos quince (15) días de antelación.
- En caso de cancelación, el anticipo no es reembolsable, salvo acuerdo previo entre ambas partes.

Confidencialidad

- Ambas partes se comprometen a mantener la confidencialidad de toda la información intercambiada en relación con esta propuesta comercial.

Propiedad intelectual

- Los derechos de propiedad intelectual de cualquier diseño, desarrollo o entrega específica quedarán bajo propiedad de E & C INGENIEROS S.A.S hasta el pago total del servicio.