

DataSec

COMISIÓN DE REGULACIÓN DE COMUNICACIONES

PROPUESTA COMERCIAL

Bogotá, D.C., 09 de julio de 2026

www.datasec.com.co

comercial@datasec.com.co

+57 320 380 5020

DataSec

TABLA DE CONTENIDO

1. PRESENTACIÓN. 3
2. CONFIDENCIALIDAD DEL DOCUMENTO. 5
3. USO Y DIVULGACIÓN. 5
4. NUESTRA EXPERIENCIA. 5
5. CERTIFICACIONES E INGENIERIA. 6
6. PROPUESTA ECONÓMICA. 8
8. EXCLUSIONES DEL SERVICIO 10
9. DISCLAIMER 10
10. OBLIGACIONES DE LOS CLIENTES 11
11. CONTROL DE CAMBIOS 12

1. PRESENTACIÓN.

Bogotá D.C., julio 09 de 2026.

Señores
COMISIÓN DE REGULACIÓN DE COMUNICACIONES

Referencia: Servicio de Hacking Ético.

Estimados señores:

DataSec S.A.S., es una compañía 100% colombiana integradora de tecnología y servicios, con un claro enfoque en las necesidades del cliente y el manejo integral de los proyectos. Contamos con un equipo de trabajo capacitado y certificado con los más altos niveles requeridos por los fabricantes, lo que nos permite llegar con soluciones a la medida a cada uno de nuestros clientes.

En DataSec S.A.S. trabajamos para convertirnos en aliados estratégicos para su negocio, generando relaciones de confianza duraderas que nos beneficien a ambos. Basados en nuestra experiencia, ofrecemos servicios de alta calidad que se ajustan a sus necesidades de manejo de información, con oportunidad y confiabilidad.

Esperamos poder participar activamente de su proceso de selección y ante cualquier inquietud estaremos atentos.

Cordialmente,

DIANA MARCELA PRADA M.
Gerente de Cuenta
Email: diana.prada@datasec.com.co
Tel: +57 3227016782

Formato	Código: FOR-COM-004
Oferta compleja	Versión: 1
	Fecha: 14/05/2025

DataSec

ACERCA DE DATASEC

Capacitaciones

Entrenamiento especializado en seguridad informática para proteger sistemas críticos y habilidades.

- Fortalecimiento de la seguridad
- Conciencia aumentada
- Prevención de incidentes

A Cyber Analítica

La ciberseguridad con inteligencia artificial detecta y mitiga amenazas en tiempo real de manera eficaz.

- Respuesta automática a incidentes
- Protección contra amenazas
- Mejora de resiliencia cibernética

Servicios Profesionales

Nuestros servicios de ciberseguridad protegen su infraestructura digital frente a amenazas y vulnerabilidades.

- Experiencia Especializada
- Prevención de brechas
- Cumplimiento normativo

Protección de Riesgos Digitales

Utiliza un equipo profesional y SaaS para monitorear marcas y evaluar los riesgos de exposición.

- Evitar suplantación de identidad
- Reputación de marca
- Reducción de riesgos legales

Centro de Operaciones de Ciberseguridad

Prevención, detección y respuesta a incidentes. Monitoreo y análisis continuos en tiempo real, 7x24.

- Detección de amenazas
- Monitoreo y vigilancia continua
- Gestión de riesgos cibernéticos

Gestión de Vulnerabilidad

Utiliza escaneo activo y monitoreo para obtener visibilidad continua y unificación de actividades.

- Reducción de ataques
- Identificación de vulnerabilidades
- Priorización de riesgo

Soluciones de Ciberseguridad

Ciberseguridad IT/OT - Ciberseguridad Cloud - Ciberseguridad Aplicaciones.

- Detección y respuesta a amenazas
- Seguridad Integral
- Adaptación a nuevas amenazas

Validación de postura en seguridad

Gestión continua y evaluación de ciberseguridad, garantizando la seguridad frente a amenazas.

- Evaluación de gestión de riesgos
- Búsqueda de eslabones débiles
- Medición de ROI e inversión

CSIRT Cyber Security Incident Response Team

Equipo de respuesta a incidentes que identifica y recupera eventos de seguridad cibernética.

- Gestión de información
- Continuidad del negocio
- Respuesta rápida a incidentes

Haz clic aquí y conoce mas de nuestros servicios.

CERTIFICACIONES Y MEMBRESÍA:

ISO 27001
LL-C (Certification)

FIRST
Improving Security Together

www.datasec.com.co

comercial@datasec.com.co

+57 320 380 5020

2. CONFIDENCIALIDAD DEL DOCUMENTO.

Este documento ha sido preparado para la presentación de nuestros servicios. Los servicios indicados en el presente documento han sido diseñados exclusivamente para ser prestados a **COMISIÓN DE REGULACIÓN DE COMUNICACIONES** y 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 de **COMISIÓN DE REGULACIÓN DE COMUNICACIONES.** Colombia y no debe ser duplicada, usada o divulgada completamente o en parte, con propósitos distintos a su evaluación.

3. USO Y DIVULGACIÓN.

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 DataSec S.A.S., catalogada como propiedad intelectual. Esta información es entregada a **COMISIÓN DE REGULACIÓN DE COMUNICACIONES,** en el entendimiento de que no será utilizada para otros fines que no sean la evaluación y control de esta propuesta.

Todos los derechos son reservados, ninguna parte de este documento puede ser fotocopiada, reproducida, divulgada o traducida sin la autorización expresa de DataSec S.A.S.

4. NUESTRA EXPERIENCIA.

Actualmente DataSec S.A.S. ha venido desempeñando un rol importante a nivel público y privado para Colombia en el campo de la ciberseguridad, contando con clientes de alto impacto a nivel nacional dando el reconocimiento al esfuerzo, ética y dedicación que entregamos a cada uno de nuestros proyectos.

DataSec

PROYECTOS NIVEL NGSOC

5. CERTIFICACIONES E INGENIERIA.

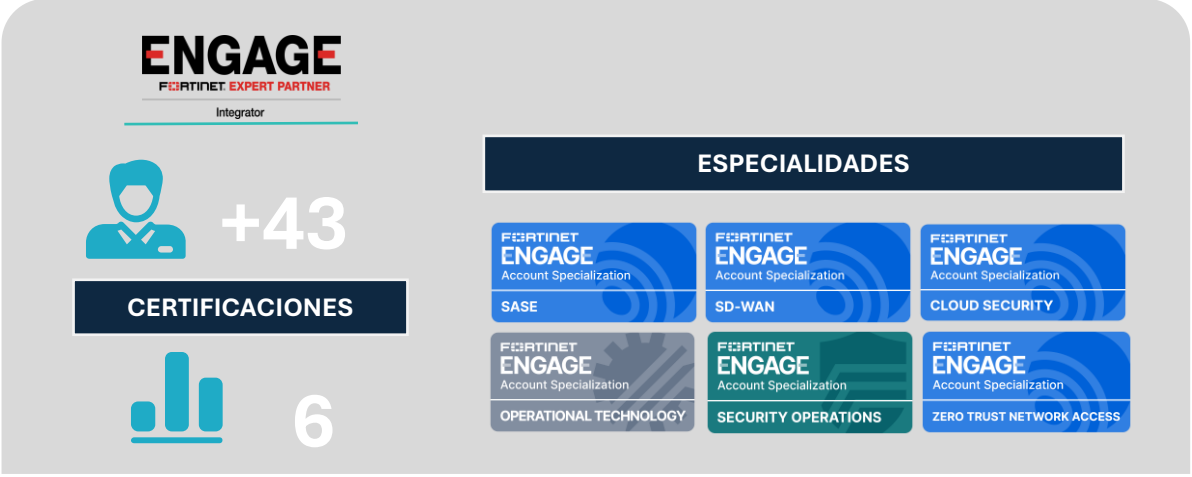
CERTIFICACIONES DEL EQUIPO DE TRABAJO.

CERTFICACIONES ESPECIALIZADAS POR FABRICANTE

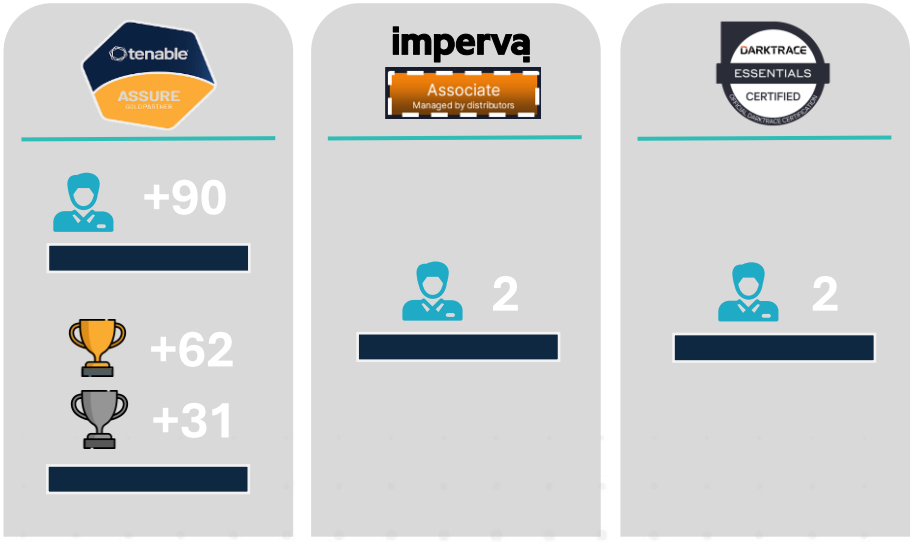
DataSec S.A.S., al ser un canal especializado en servicios profesionales cuenta con las certificaciones y membresías del más alto nivel en FORTINET, denotando así, compromiso, responsabilidad y conocimiento en una de las empresas más importantes a nivel mundial en el sector de la ciberseguridad, que ofrece soluciones completas impulsadas por los mejores avances en tecnología, incluyendo la inteligencia artificial.

DataSec

DataSec S.A.S. cuenta con ingenieros especialistas certificados en la marca con la que construimos confianza con nuestros clientes, a raíz de la experiencia en el sector tecnológico. Actualmente somos partner EXPERT (La más alta membresía en FORTINET) al poder ejecutar proyectos de gran relevancia a nivel nacional y con la máxima calidad de trabajo.



CERTIFICACIONES DE OTRAS MARCAS



DataSec

6. PROPUESTA ECONÓMICA.

SERVICIO DE HACKING ÉTICO				
ITEM	**CONCEPTO**	**UNIDAD**	**VALOR UNITARIO**	**VALOR TOTAL**
1	Pentesting automatizado para 90 Ips incluido retest.	1	$ 30.000.000	$ 30.000.000
2	Acompañamiento informe y presentación de reultados.	1	$ 7.000.000	$ 7.000.000
SUBTOTAL				$ 37.000.000
IVA				$ 7.030.000
TOTAL				$ 44.030.000

ALCANCE TÉCNICO

La oferta presentada contempla, una fase de pruebas de seguridad, en la cual se llevará a cabo un ejercicio de pruebas de penetración (pentest) sobre un máximo de 90 direcciones IP. Estas IP serán previamente identificadas, priorizadas y asignadas por el cliente, garantizando que el alcance del análisis responda a sus necesidades específicas de evaluación y fortalecimiento de su postura de ciberseguridad

Exploración	La solución de penetración sondea una red determinada mediante la identificación de direcciones IP activas, puertos y detalles de topología y descubrimiento de todos los hosts, servidores y dispositivos relacionados. Ver detalle de los métodos y TTPs luego de esta tabla.
Enumeración	La solución de penetración extrae datos del equipo, datos de usuario, nombres de host, recursos / recursos compartidos de red, sistema de archivos y otros servicios creando una conexión activa a un sistema determinado. Ver detalle de los métodos y TTPs luego de esta tabla.
Evaluación Vulnerabilidad	La solución de penetración escanea los hosts activos en busca de vulnerabilidades conocidas. Ver detalle de los métodos y TTPs luego de esta tabla.
Sniffing Credentials	La solución de penetración intercepta el tráfico de red y los datos relacionados con el host para extraer las credenciales de los usuarios con especial atención a los usuarios privilegiados, incluidas las cuentas de dominio de DA (Directorio Activo) y las cuentas locales. Ver detalle de los métodos y TTPs luego de esta tabla.
Craqueo de contraseñas	La solución de penetración utiliza varias medidas para recuperar contraseñas de texto sin formato de usuarios, hosts y servidores descifrando hash de contraseñas a partir de datos almacenados o transportados desde un sistema mediante una combinación de técnicas de diccionario y de fuerza bruta. Ver detalle de los métodos y TTPs luego de esta tabla.
Relay	La solución de penetración intercepta las comunicaciones entre dos partes y transmita los datos a otro dispositivo (de terceros), incluidas las técnicas basadas en la red MITM. Ver detalle de los métodos y TTPs luego de esta tabla.

Código remoto de ejecución	La solución de penetración utiliza varios métodos para la ejecución remota de código en un sistema determinado mediante el uso de capacidades de evasión de defensa para evitar los mecanismos de detección AV / EDR y abrir un canal C&C para controlar el ataque al dispositivo objetivo. Ver detalle de los métodos y TTPs luego de esta tabla.
Recopilación de datos	La solución de penetración reúne datos adicionales del punto final, incluidos productos de seguridad, detalles de acceso a la red, credenciales de dominio / locales, credenciales / historial del navegador, seguridad. Archivo de Gerente de Cuenta (SAM) y acceso a aplicaciones y servicios críticos en la nube / locales. Ver detalle de los métodos y TTPs luego de esta tabla.
Movimiento lateral	La solución de penetración administra un procedimiento de extracción dedicado de material de autenticación para poder pivotar lateralmente a nuevos puntos finales en la red. Ver detalle de los métodos y TTPs luego de esta tabla.
Escalada de privilegios	La solución de penetración posee capacidades remotas y locales para escalar de un usuario sin privilegios a poder ejecutar código con altos permisos. Ver detalle de los métodos y TTPs luego de esta tabla.
Exfiltración de datos	La solución de penetración verifica la transferencia de datos desde un punto final de destino desencadenada por la adquisición de un dispositivo. Ver detalle de los métodos y TTPs luego de esta tabla.
Limpieza	La solución de penetración realiza la limpieza de los residuos creados por el ataque. Ver detalle de los métodos y TTPs luego de esta tabla.

Exploración (Scanning)

Se sondea la red identificando direcciones IP activas, puertos y detalles de topología y descubriendo todos los hosts, servidores y dispositivos relacionados.

Métodos	TTPs Relacionados
Descubrimiento de contenedores de Azure usando la API de Microsoft	Descubrimiento de Cuentas (T1087)
Descubrir hosts activos usando variantes del protocolo ARP para lograr máxima sigilosidad	Escaneo Activo (T1595)
Descubrir dispositivos activos basándose en aplicaciones comunes y el análisis de sus respuestas	Descubrimiento de Infraestructura en la Nube (T1580)
Aprovechar protocolos broadcast y multicast para activar respuestas desde endpoints vecinos	Descubrimiento de Servicios en la Nube (T1526)
Utilizar protocolos de capa 3 (L3) para cruzar fronteras hacia nuevos segmentos de red mediante variantes de ICMP, SCTP y protocolos multicast	Descubrimiento de Confianza de Dominio (T1482), Recolección de Información de la Víctima (T1590), Escaneo de Servicios de Red (T1046), Descubrimiento de Recursos Compartidos en Red (T1135), Sniffing de Red (T1040)
La solucion ofertada permite controlar el Nivel de Sigilosidad de cada escenario de prueba para definir el nivel de ruido y agresividad del test de penetración	Descubrimiento de Políticas de Contraseñas (T1201), Descubrimiento de Grupos con Permisos (T1069), Descubrimiento de Sistemas Remotos (T1018), Descubrimiento de Información del Sistema (T1082), Descubrimiento de Configuración de Red del Sistema (T1016), Descubrimiento de Conexiones de Red del Sistema (T1049)

NOTA: el cliente tendra 3 meses a partir de la entrega del informe de los hallazgo para hacer la remedición, una vez se cumpla los 3 meses se procede a realizar el retest, si no se hace en este tiempo no se responderá por dicha actividad.

Términos y Condiciones.

- Los precios están expresados en Pesos colombianos.
- La oferta tiene una vigencia de 30 días a partir de la fecha de presentación.
- La entrega de los equipos en la ciudad de Bogotá para compra es de 10 días máximo, para la opción de renting se revisará la disponibilidad con el mayorista.
- Servicios Cloud no adiciona IVA al costo.
- Entrega de 3 días hábiles.
- Los servicios se prestarán de manera presencial en la ciudad de Bogotá D.C., en caso de requerirse presencialidad en otras ciudades fuera de Bogotá D.C. esta propuesta no incluye costos de traslados, desplazamientos, viáticos y/o servicio de manos remota, los servicios se prestarán de manera remota por sesión virtual.

Forma de pago.

- 50% como anticipo y 50% restante a la entrega del informe.

8. EXCLUSIONES DEL SERVICIO

EL SERVICIO NO INCLUYE:

- Cualquier actividad *que no haya sido incluida explícitamente en la oferta, no se considera dentro del alcance de esta,* tales como: Costos de licenciamientos o garantías de fabricante, diagnóstico de problemas ajenos a la solución o tecnología ofertada, la interacción y configuración, afinamiento y/o consultas técnicas diferentes a las de los productos, plataformas o dispositivos relacionadas en la propuesta o de terceros no contemplados en el alcance, parametrización y/o construcción de analítica, intervención y/o reemplazo de equipos que estén fuera del soporte y garantías con el fabricante, entre otras.
- Servicios profesionales o de instalación de puntos de red o eléctricos, adecuación del cableado estructurado, obra civil, transporte de equipos, recursos de máquina virtual, almacenamiento de información y/o canales de telecomunicaciones como Internet, MPLS y/o medios satelitales.
- Configuraciones y/o recomendaciones de la infraestructura tecnológica de recursos computacional.
- Implementación, configuración y puesta en marcha de los hipervisores contemplados en el despliegue final de la arquitectura.
- Afinamiento de políticas que no representen un incidente. Servicios de reposicionamiento o estudios de site survey para las plataformas wifi.

9. DISCLAIMER

- Si por razones ajenas a DataSec S.A.S., las actividades son canceladas o quedan incompletas, se dejará constancia en un acta que deberá firmar el encargado del Cliente que esté en sitio en el momento de los sucesos.

- El resultado de un apoyo programado que resulte en actividades nuevas sobre equipos ajenos a la solución no será ejecutado.
- La instalación se realizará de manera remota o presencial (de acuerdo con lo plasmado en la preventa comercial).
- La solución a incidentes está relacionada con el soporte a fallo.
- La atención en sitio solo cubre la ciudad de Bogotá D.C., y se realizará atención en sitio, solo si la situación lo requiere.
- Recomendaciones y buenas prácticas se contemplan en la bolsa de horas dimensionada en la propuesta económica.
- Los informes de gestión del proyecto se realizarán una vez que se realice algún tipo de soporte o se haga uso de la bolsa de horas.
- **Solicitudes de auditorías por parte del cliente:** Las auditorías a los procesos de DataSec S.A.S., serán con el alcance para verificar el cumplimiento de los Acuerdos de Niveles de Servicio (SLA) definidos junto con el cliente específico, según los compromisos contractuales.
  El ejercicio de auditoría será planeado y acordado entre DataSec S.A.S. y el cliente, y no se dará acceso a la información clasificada como Confidencial, de acuerdo con el Sistema de Gestión de Seguridad de la Información ISO 27001.

10. OBLIGACIONES DE LOS CLIENTES

- Realizar la comunicación interna para dar inicio al proyecto.
- Proporcionar el levantamiento de información para dar viabilidad a los servicios a prestar.
- Asegurar que el dispositivo es usado bajo las recomendaciones proporcionadas por el fabricante. DataSec S.A.S. no es responsable de soportar dispositivos o productos de terceros.
- Mantener los contratos de soporte y garantías de los dispositivos de terceros.
- Mantener los dispositivos en las versiones estables más recientes de acuerdo con las recomendaciones del fabricante.
- Proveer la conectividad necesaria y los accesos para brindar al Ingeniero de implementación y soporte de DataSec S.A.S., la entrada necesaria al dispositivo.
- En ninguna circunstancia, los Ingenieros de DataSec S.A.S. se conectarán a los dispositivos sin la autorización del cliente, y solo se conectarán para temas relacionados con el soporte de acuerdo con los requerimientos de la entidad.
- Proveer las condiciones físicas que cumplan con la legislación vigente en seguridad y salud en el trabajo, para las actividades de instalación en sitio.
- Realizar la disposición final de residuos convencionales y de residuos de aparatos eléctricos y electrónicos, de acuerdo con la legislación ambiental vigente.

11. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS DE LA OFERTA			
Versión	***Numeral***	***Descripción***	***Fecha***
1		Presentación de oferta de acuerdo con solicitud del cliente.	09/07/2026

Cordialmente,

DIANA MARCELA PRADA M.
Gerente de Cuenta
Email: diana.prada@datasec.com.co
Tel: +57 3227016782

FIN DEL DOCUMENTO