a3sec

‹BLINDAMOS ACTIVOS DIGITALES GLOBALMENTE›

Estudio de Mercado para:

PROPUESTA DE SERVICIO
Análisis de vulnerabilidades y hacking ético

< ESPAÑA / MÉXICO / COLOMBIA / ECUADOR>
Colombia, 15 JULIO 2026
Versión #1 .0

< Blindamos activos digitales globalmente />

< Documento confidencial />

Derechos de uso

La presente documentación tiene carácter de confidencialidad y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de A3Sec.

Señores
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Atn. Juan Nicolás Ayala Rodriguez

ASUNTO: Cotización Servicio, Análisis de vulnerabilidades y hacking ético

Estimado, reciba mis saludos,

Agradezco la confianza depositada en Grupo A3Sec, para nosotros es un placer poner nuestras soluciones a su servicio. A continuación, se describe el alcance de la propuesta y el valor de nuestra solución, junto a las condiciones comerciales necesarias para la negociación.

Quedo a su entera disposición para aclarar cualquier inquietud referente a nuestra propuesta, no dude en comunicarse con nosotros para atenderlo inmediatamente.

Cordialmente,



SANDRA P. GARCÍA M.
ACCOUNT MANAGER
E. sandra.garcia@A3Sec.com
M. +57 317423 1770

>_ CONTENIDO

1. INTRODUCCIÓN **5**

1.1 Perfil de A3Sec 5

1.1.2 Operación de Seguridad Unificada 6

1.1.3 Certificaciones obtenidas 7

1.1.4 ¿Cómo lo logra CSVD by A3Sec? 8

2. ANTECEDENTES **9**

3. PROPUESTA TÉCNICA **10**

3.1 Información de la solución propuesta 10

3.4 Entregables 16

3.5 Metodología de proyectos 17

3.6 Propuesta Económica 21

3.7 Condiciones comerciales 22

3.8 Limitaciones técnicas y exclusiones del servicio 22

3.9 Condiciones generales para la prestación del servicio 23

3.11 Servicios adicionales 23

4. ACEPTACIÓN DEL PEDIDO **24**

1. INTRODUCCIÓN

El presente documento presenta la Oferta emitida por Grupo A3Sec a la **Comisión de Regulación de Comunicaciones** en adelante **(CRC).** para el suministro del servicio de Análisis de vulnerabilidades y hacking ético.

1.1 Perfil de A3Sec

Grupo A3Sec es una firma global de ciberseguridad que impulsa a las organizaciones a evolucionar de la resiliencia a la **ciber-antifragilidad**: la capacidad no solo de resistir los ataques, sino de anticiparse a ellos y salir fortalecidas. Con más de 12 años de trayectoria y un equipo de más de 150 expertos operando en España, México, Colombia y Ecuador, la compañía combina inteligencia de amenazas y metodologías avanzadas de seguridad ofensiva.

Nuestra propuesta de valor en **Análisis de Vulnerabilidades** va más allá del simple escaneo automatizado; aplicamos un enfoque holístico —que cubre host, identidad, nube, entornos IT/OT y red— para descubrir, clasificar y priorizar brechas reales de seguridad. Este diagnóstico proactivo permite a nuestros clientes **reducir su superficie de exposición en más de un 73%** durante los primeros ejercicios, transformando el conocimiento de sus propias debilidades técnicas en una ventaja competitiva y en un escudo de defensa impenetrable.



1.1.2 Operación de Seguridad Unificada

A3Sec cuenta con un **Centro de Seguridad y Vigilancia Digital**. Más que una solución tecnológica, es un equipo de guerreros digitales, con herramientas avanzadas para BLINDAR los activos digitales.

Pilares diferenciales

1. **Data driven:** Buscamos resolver el reto de los altos costos que representan procesar y almacenar información necesaria para la operación de seguridad a través de un datos federados que reduce el tamaño del log, enrique los datos y almacena toda la información para cumplimiento o cacería de amenazas a costos muy competitivos.

2. **Inteligencia:** Partimos de la premisa que es necesario primero conocernos a nosotros mismos identificando los indicadores de exposición, luego conocer a nuestros adversarios a través de los indicadores de ataque para poder identificar aquellos indicadores de compromiso que puedan alertarnos sobre un posible ataque.

3. **Hiper Automatización:** Un enfoque completo orientado hacia orquestación de procesos para la automatización de la gestión de activos, incidentes, configuraciones, riesgos y servicios en búsqueda de reducir el dwell time en la atención de incidentes.

4. **Mejora continua:** Contamos con tanques de pensamiento que se alimentan del feedback de nuestros clientes, donde se analizan los nuevos requerimientos realizando una evaluación técnica, económica y de mercado hasta culminar en el desarrollo de un nuevo producto o funcionalidad.

5. **Estrategia:** Trabajamos alineados a estándares internacionales y usamos como marco de referencia Framework [NIST 2.0].

1.1.3 Certificaciones obtenidas

ISO 22301: Norma internacional para la Gestión de la Continuidad de Negocio (SGCN) que está diseñada para ayudar a las organizaciones a prevenir, preparar, responder y recuperarse de incidentes inesperados.

ISO 20000: Norma Internacional que especifica los requisitos para un sistema eficaz de gestión de servicios de tecnología de la información (ITSM). Este estándar se utiliza para establecer, implementar, mantener y mejorar un sistema de gestión de servicios que garantice la calidad de los servicios de TI.

ISO 27017: Norma Internacional de buenas prácticas de seguridad de la información para servicios en la nube. Esta norma proporciona controles de seguridad adicionales tanto para los proveedores de servicios en la nube como para los clientes de servicios en la nube.

ISO 27001: Norma internacional cuyo objetivo es establecer un sistema de gestión de la seguridad de la información (SGSI) para garantizar la accesibilidad, confidencialidad e integridad continuas de la seguridad de la información.

ISO 9001: Norma internacional que establece un Sistema de Gestión de Calidad (SGC) para las organizaciones. Al cumplir con los requisitos propuestos, garantiza que el desempeño de la actividad de la organización está orientado a la mejora continua y que los productos y servicios suministrados satisfacen al cliente.

ENS: El Esquema Nacional de Seguridad (ENS), asegura el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos e información utilizados por medios electrónicos en el ejercicio de sus competencias

SOC 1 Type 1: El informe SOC 1 se centra en los controles internos relacionados con la información financiera. Evalúa los controles de un proveedor de servicios que impactan los estados financieros de sus clientes.

SOC 2 Type 1: El informe SOC 2 se centra en los controles relacionados con la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y la privacidad. Evalúa los controles de un proveedor de servicios que protegen los datos y la información sensible de sus clientes.

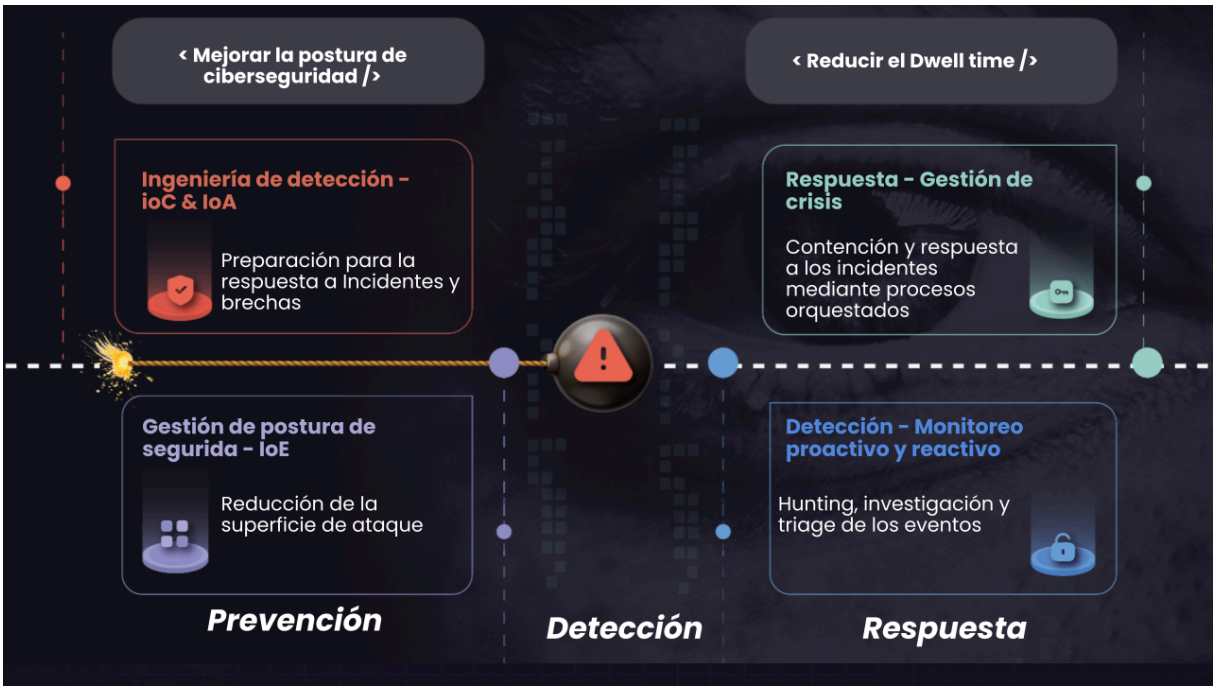
SOC 3 Type 1: El informe SOC 3 es una versión simplificada y disponible públicamente del informe SOC 2. Proporciona una descripción general del sistema del proveedor de servicios y los controles establecidos para respaldar la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y la privacidad.

FIRST: FIRST reúne una amplia variedad de equipos de seguridad y respuesta a incidentes, incluidos equipos de seguridad de los sectores gobierno, comercial y académico.

1.1.4 ¿Cómo lo logra CSVD by A3Sec?

Los riesgos cibernéticos generan la necesidad latente de contar con una solución para la postura de seguridad digital, que pueda contrarrestar los ataques en tiempo real.

- **Prevención:** Revisa y gestiona las posibles vulnerabilidades del sistema, anticipando ataques para cerrar brechas y mejorar la postura de seguridad.
- **Detección:** Analiza intromisiones y movimientos investigando amenazas usando analítica de datos y machine learning.
- **Reacción:** Reacciona de forma inmediata ante los atacantes por medio de la seguridad en profundidad fundamentada en hiperautomatización.



2. ANTECEDENTES

Actualmente en la **CRC** requieren una propuesta para cotizar un servicio de análisis de vulnerabilidades y Ethical Hacking. El servicio se ejecutará bajo un enfoque metodológico estructurado en las siguientes actividades:

- Realizar el levantamiento de información necesaria.
- Elaborar y presentar el plan de trabajo para la aplicación de las pruebas a nivel de usuario sin privilegios y con privilegios teniendo en cuenta su arquitectura si cuenta con alta disponibilidad o no y sus ambientes de pruebas y producción.
- Ejecutar pruebas de penetración internas hasta 90 IP o fuentes.
- Realizar el análisis de resultados y presentar un informe de las pruebas realizadas que incluya "Descripción, Vulnerabilidad, valoración, criticidad, Impacto, Recomendaciones a seguir" y realizar el diagnóstico y presentar las recomendaciones sobre el nivel de aseguramiento de los componentes de la red de la CRC.

- Realizar la evaluación del esquema de seguridad de las bases de datos que la CRC utiliza internamente para su operación.
- Realizar la evaluación de la vulnerabilidad de los sitios INTERNOS de la entidad.

Una vez terminada las pruebas se debe presentar a la CRC el análisis de resultados.

- Presentar las recomendaciones a implementar para solucionar cada uno de los elementos analizados, indicando el nivel de impacto en tiempo y costo.
- Presentar un plan de remediación con prioridades, a ser adelantado por la CRC, determinando las acciones de corto, mediano y largo plazo de acuerdo con resultado del análisis de vulnerabilidades.

3. PROPUESTA TÉCNICA

3.1 Información de la solución propuesta

Objetivo del Servicio Fortalecer la postura de seguridad de la información del cliente mediante la identificación, análisis y explotación controlada de vulnerabilidades en sus activos tecnológicos, simulando escenarios reales de ataque con el fin de validar la efectividad de los controles existentes, reducir la superficie de exposición y entregar recomendaciones accionables que soporten la toma de decisiones en materia de ciberseguridad.

Alcance del Servicio Ejecución de pruebas modalidad caja negra a:
Los servicios ofertados comprenden la ejecución de pruebas de seguridad ofensiva sobre la infraestructura tecnológica, aplicaciones y controles perimetrales del cliente, incluyendo:

- Análisis de Vulnerabilidades a 90 activos
- Ethical Hacking (Caja Gris) a 90 activos
- Ethical Hacking (Caja Gris) a máximo 5 portales web transaccionales

- Evaluación del esquema de seguridad de máximo 2 bases de datos internas

Se incluye un retest sin costo adicional sobre los mismos activos evaluados en la prueba inicial, siempre que sea solicitado y ejecutado dentro de los cuatro (4) meses siguientes a la finalización de las pruebas.

Prerrequisitos Para la ejecución del servicio se requiere lo siguiente:
Para garantizar la correcta ejecución de los servicios, el cliente deberá suministrar, según aplique para cada ejercicio:

- Dirección IP y/o URL de los activos expuestos a internet que serán evaluados.
- Acceso VPN a una VLAN con visibilidad sobre los activos internos en alcance.
- Colecciones de APIs (Postman o equivalente) para las evaluaciones sobre APIs.
- Aplicación disponible en tienda o archivo APK/IPA para evaluaciones móviles.
- Ventana de mantenimiento acordada para la ejecución de la consultoría y revisión técnica del Firewall, con respaldo de configuración realizada previamente por el cliente.
- Autorización de acceso a instalaciones físicas para pruebas en sitio, cuando aplique.
- Carta de autorización firmada por el representante legal, habilitando la ejecución de las pruebas.

Enfoque metodológico Pentesting
Nuestra metodología integra la experiencia técnica de nuestros especialistas con los estándares internacionales, garantizando una cobertura exhaustiva frente a amenazas emergentes. Entendemos que la seguridad no es un fin en sí mismo, sino un habilitador del negocio. Por ello, nuestra evaluación trasciende el análisis técnico tradicional integrando escenarios de riesgo específicos para su organización. Esto nos permite medir el impacto real de una brecha en la

continuidad operativa, priorizando los hallazgos según su criticidad para sus activos más valiosos.

Este enfoque, respaldado por nuestra trayectoria a través de diversos sectores industriales, nos permite ofrecer una visión alineada con las amenazas recurrentes de su mercado, transformando hallazgos técnicos en planes de mitigación claros y accionables para la toma de decisiones.

Para garantizar una detección temprana de amenazas, operamos bajo un modelo de fases que nos permite identificar brechas en cada etapa de la cadena de ataque. Este proceso asegura que la postura de seguridad de la organización se fortalezca de manera progresiva, como se ilustra a continuación:



Empleamos una metodología estructurada, reproducible y basada en riesgo para la ejecución de todos sus servicios de seguridad ofensiva. El proceso se organiza en cuatro fases secuenciales que garantizan cobertura integral, trazabilidad y alineación con los objetivos de negocio del cliente:

Fase 1 – Reconocimiento e Inteligencia: Se recopila información pasiva y activa sobre los activos en alcance direccionamiento IP, dominios, tecnologías expuestas, usuarios, configuraciones y superficie de ataque. Esta fase permite construir un modelo de amenaza específico para la organización antes de iniciar la explotación.

Fase 2 – Escaneo y Enumeración: Se ejecutan escaneos automatizados complementados con revisión manual profunda. Los hallazgos se validan y

correlacionan con los marcos internacionales aplicables (CVE, NVD, OWASP, CIS Benchmarks) para eliminar falsos positivos y garantizar precisión en los resultados.

Fase 3 – Explotación Controlada Las vulnerabilidades confirmadas el equipo procede a explotarlas de forma segura y deliberada para demostrar su impacto real. Se emplean técnicas manuales y herramientas especializadas para obtener acceso a los sistemas afectados, evitando en todo momento acciones que puedan comprometer la estabilidad o disponibilidad del entorno productivo. Los resultados de esta fase alimentan directamente el plan de remediación, transformando cada hallazgo técnico en un riesgo concreto y medible para el negocio.

Fase 4 – Post-Explotación: Una vez confirmado el acceso inicial, el equipo evalúa el alcance real del compromiso. Se realizan actividades de movimiento lateral entre segmentos de red, escalación de privilegios hacia cuentas de mayor jerarquía y, cuando el alcance lo permite, acceso a activos críticos como controladores de dominio, bases de datos o repositorios de información sensible. Todas las acciones se ejecutan de forma controlada, sin afectar la disponibilidad de los sistemas productivos, y quedan documentadas con evidencia técnica.

Cobertura técnica por capa del ecosistema digital

Nuestra capacidad de análisis no es genérica; adaptamos cada evaluación a la naturaleza tecnológica de los activos. Para asegurar el máximo rigor técnico, fundamentamos nuestras pruebas en los marcos de trabajo y estándares internacionales de la industria, garantizando una cobertura integral en cada capa de su ecosistema digital:

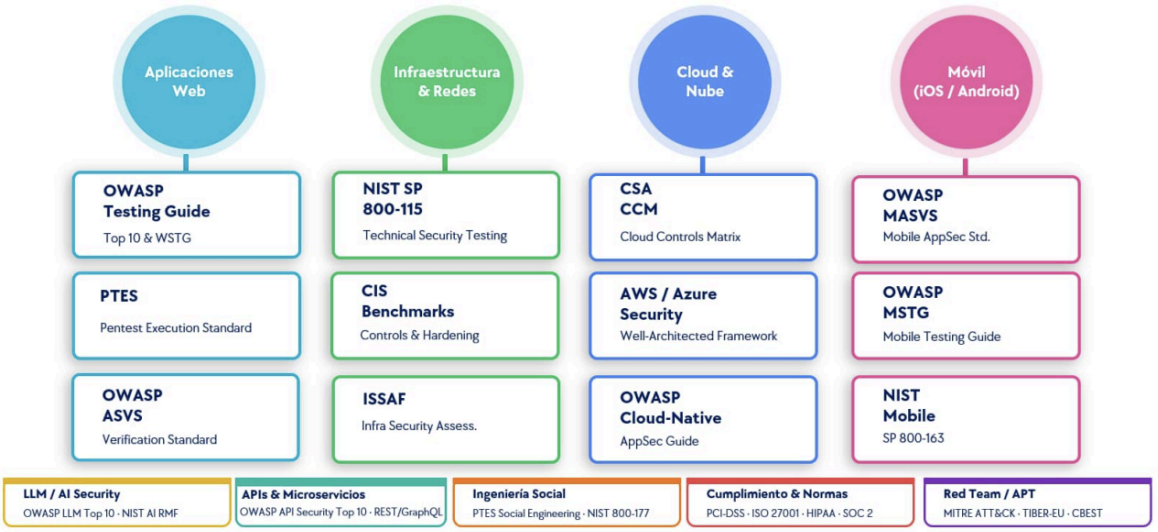
Aplicaciones Web & APIs: Aplicamos los estándares de OWASP (WSTG, ASVS, API Security) para identificar vulnerabilidades críticas en el software.

Infraestructura y Redes: Nos basamos en NIST SP 800-115 y CIS Benchmarks para evaluar la robustez de sus servidores y comunicaciones.

Cloud & Nube: Aseguramos entornos modernos mediante la Cloud Controls Matrix (CCM) de la CSA y los marcos de arquitectura segura de AWS y Azure.

Seguridad Móvil: Evaluamos apps en iOS y Android bajo el estándar OWASP MASVS/MSTG y guías de NIST Mobile.

Escenarios Avanzados: Integramos pruebas de Red Team (MITRE ATT&CK), ingeniería social y seguridad en Inteligencia Artificial (LLM / AI Security), asegurando el cumplimiento con normativas como ISO 27001, PCI-DSS y SOC 2.



Evaluación de la severidad

Cada vulnerabilidad identificada es evaluada mediante el Common Vulnerability Scoring System versión 3.1 (CVSS v3.1), que permite obtener una puntuación objetiva y reproducible basada en los siguientes vectores:

Base Score: evalúa características intrínsecas de la vulnerabilidad: vector de ataque, complejidad, privilegios requeridos, interacción del usuario, alcance e impacto sobre Confidencialidad, Integridad y Disponibilidad (CIA).

Temporal Score: ajusta la puntuación base según la madurez del exploit disponible, nivel de remediación y confianza en el reporte.

Environmental Score: personaliza la puntuación según los requisitos de seguridad específicos de la organización y la criticidad del activo afectado. La escala de severidad resultante se define así:

Nivel de severidad Crítica (9.0 – 10): Corresponde a la vulnerabilidad que permitiría a un atacante informático el ingreso total de la máquina violando todos los principios de seguridad de la información como confidencialidad, integridad y disponibilidad de toda la infraestructura.

Nivel de severidad Alta (7.0 – 8.9): Corresponde a vulnerabilidades mediante el cual un intruso podría generar una afectación a la máquina, pero con algunas limitantes a la hora de la ejecución del ataque y obtención de privilegios del sistema, aquellas vulnerabilidades altas también se refieren a vulnerabilidades que no tienen exploits disponibles o la ejecución del ataque no se lleva a cabo de manera automática.

Nivel de severidad Media (4.0 – 6.9): corresponde a las vulnerabilidades por medio de las cuales es posible obtener acceso a información específica almacenada en los dispositivos, incluyendo configuraciones de seguridad. Las vulnerabilidades de este tipo incluyen la divulgación de contenido de archivos, divulgación de reglas de filtrado y mecanismos de seguridad, uso de servicios sin autorización, entre otros.

Nivel de severidad Baja (0.1 – 3.9): corresponde a las vulnerabilidades por medio de las cuales un intruso puede recolectar información de los dispositivos (Sistema Operativo, puertos abiertos, servicios, etc.), posiblemente se puede usar dicha información para buscar otras vulnerabilidades.

	Facilidad de Explotación		
Evaluación del Impacto	Alto	Medio	Bajo
Crítico	Severidad Crítica	Severidad Crítica	Severidad Alta
Alto	Severidad Alta	Severidad Alta	Severidad Media
Medio	Severidad Alta	Severidad Media	Severidad Baja
Bajo	Severidad Media	Severidad Baja	Severidad Baja

Ajuste Contextual – Riesgo para el Negocio

La puntuación CVSS es un punto de partida técnico, pero no refleja por sí sola el impacto real en el negocio. Por ello, aplicamos los siguientes factores de ajuste contextual:

Criticidad del activo afectado: un hallazgo de severidad Media en un servidor de base de datos que almacena información financiera regulada puede ser tratado como Alta por su impacto potencial en el negocio.
Exposición y accesibilidad: vulnerabilidades explotables desde Internet sin autenticación reciben prioridad superior a las que requieren acceso interno privilegiado.
Disponibilidad de exploit: si existe un exploit público maduro (Metasploit, PoC en GitHub), la urgencia de remediación se incrementa independientemente del score base.
Impacto regulatorio y de cumplimiento: hallazgos que afectan controles regulatorios (PCI-DSS, ISO 27001, Ley 1581) son escalados en prioridad dado su impacto en multas y sanciones.
Encadenamiento de vulnerabilidades: se identifican y documentan cadenas de ataque donde la combinación de hallazgos de baja severidad puede resultar en un impacto crítico.

3.4 Entregables

A continuación, se describen los entregables que se generan como resultado de las pruebas realizadas:

A. El informe ejecutivo presentará un resumen gerencial de las pruebas realizadas, incluyendo los hallazgos identificados con su nivel de riesgo, el impacto potencial para la organización y las recomendaciones de mitigación correspondientes acompañado de una tabla resumen de vulnerabilidades priorizadas por nivel de riesgo.

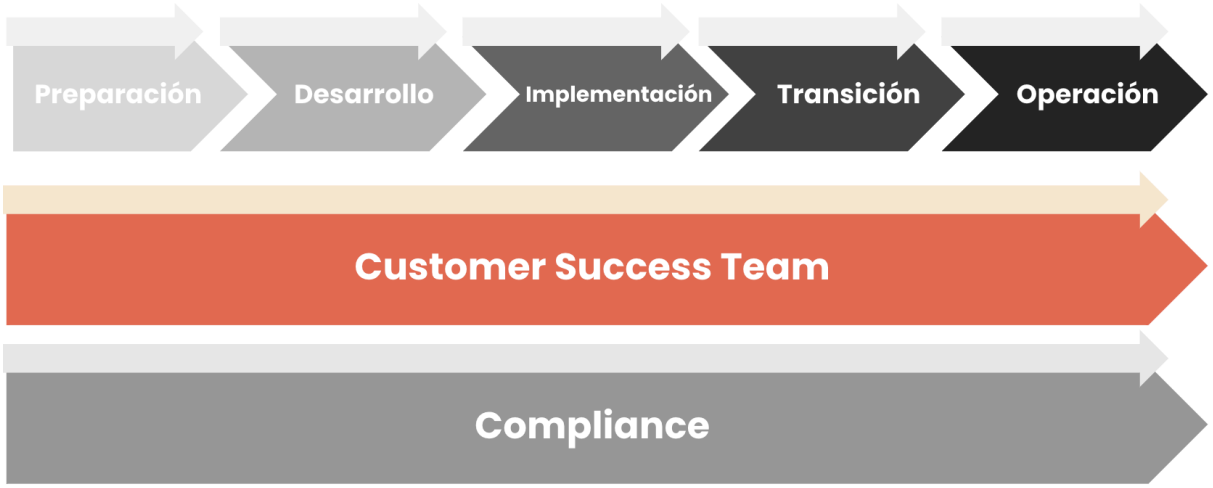
B. El informe técnico detallará cada vulnerabilidad identificada, incluyendo su descripción, nivel de severidad, evidencia, vectores de explotación, referencias técnicas de soporte y recomendaciones detalladas para su mitigación.

C. El Informe de retest (cuando aplica) contempla la verificación del estado de las vulnerabilidades reportadas en el informe original, indicando cuáles fueron remediadas y cuáles permanecen abiertas.
D. Los informes serán entregados dentro de los siete (7) días hábiles siguientes a la finalización del ejercicio.
E. Los entregables se considerarán aceptados si dentro de los cinco (5) días hábiles siguientes a su entrega no se reciben observaciones formales por escrito.

3.5 Metodología de proyectos

Como parte de las actividades de mejora continua de A3Sec, y en línea con los objetivos estratégicos de la compañía asociados con el proceso de relación con el cliente, se estableció un equipo de trabajo llamado **CUSTOMER SUCCESS MANAGER** que realiza un acompañamiento a los clientes de la organización y al equipo de trabajo que opera los servicios que provee A3Sec, para garantizar que se realice un correcto seguimiento a los acuerdos de nivel de servicio definidos con los clientes y su correspondiente cumplimiento.
Esto permite fortalecer la calidad de los servicios ofrecidos por A3Sec, manteniendo una constante comunicación con el cliente y el equipo de operaciones para detectar rápidamente oportunidades de mejora y apoyar el seguimiento a la ejecución de las actividades definidas en los proyectos.

El equipo de Customer Success (CS), realiza un acompañamiento transversal a las diferentes etapas de ejecución de los proyectos, apoyado en una estructura formal de proyectos con enfoque ágil, acorde a los requerimientos y ANSs del cliente..



PREPARACIÓN

Entendimiento de la Oportunidad Cerrada: Aclaración de dudas sobre el proyecto y definición de un CSM y un responsable técnico para el proyecto.

Diseño del SOW y KickOff: Diseño de documentación clave para el entendimiento del proyecto y definición del cronograma de implementación.

Sesión de KickOff con el Cliente: Se presenta al equipo de trabajo, se aclaran dudas por parte del cliente, se realizan ajustes sobre las actividades y fechas de ejecución.

Documentación y seguimiento del Proyecto: Estructuración del proyecto en la herramienta de seguimiento y control y consolidación de documentación del proyecto

Seguimiento a la firma de SOW y KickOff: Entrega de SOW y Acta de sesión de KickOff para firma, revisión, ajustes y firma de documentos por parte del equipo técnico y el cliente.

DESARROLLO

Modelo de Seguimiento de ANSs: Diseño de Estructura de ANSs definido para el proyecto y alineación de presentación de resultados al cliente

Seguimiento a actividades de desarrollo: Verificación de actividades de desarrollo, seguimiento al cumplimiento de ANSs definidos para la etapa.

Retroalimentación del cliente: Identificación de oportunidades de mejora del servicio, registro y seguimiento de planes de acción para la mejora continua.

IMPLEMENTACIÓN

Seguimiento a actividades de Implementación: Verificación de actividades de implementación, seguimiento al cumplimiento de ANSs definidos para la etapa.

Retroalimentación del cliente: Identificación de oportunidades de mejora del servicio, registro y seguimiento de planes de acción para la mejora continua

TRANSICIÓN

Estabilización del Servicio: Seguimiento a actividades de transición y acompañamiento al entendimiento de la implementación realizada.

Diseño de Memoria Técnica y Delivery Note: Diseño de documentación técnica de cierre del proyecto y diseño de acta de cierre

Cierre formal de Implementación: Presentación de cierre de la etapa de implementación y solicitud de firmas de aprobación

OPERACIÓN

Seguimiento al cumplimiento de ANSs: Verificación permanente de estado de cumplimiento de ANSs, presentación periódica ante el cliente del cumplimiento de ANSs

Seguimiento a actividades de Operación: Verificación de actividades de la operación y seguimiento a planes de trabajo y cargabilidad

Retroalimentación periódica del cliente: Sesiones personalizadas para identificar oportunidades de mejora y evaluación de NPS

3.6 Propuesta Económica

ITEM	DESCRIPCIÓN	CANT.	PRECIO DEL SERVICIO EN COP
1	**servicio de Análisis de Vulnerabilidades y Ethical Hacking para la CRC** **Incluye:** - Análisis de Vulnerabilidades a 90 activos - Ethical Hacking (Caja Gris) a 90 activos - Ethical Hacking (Caja Gris) a máximo 5 portales web transaccionales - Evaluación del esquema de seguridad de máximo dos bases de datos internas. - Customer Success para seguimiento, calidad y entrega del proyecto	1	$96,637,143

*Estos valores no incluyen IVA

3.7 Condiciones comerciales

- Valores en pesos colombianos
- La facturación se estructurará en dos momentos: el 40% del valor total deberá ser cancelado previo al inicio de las actividades, como condición para dar comienzo a la ejecución del servicio. El 60% restante se facturará una vez sean entregados los informes correspondientes. La ejecución del retest no es impedimento para la presentación y pago de la factura final. A3Sec S.A.S. se reserva el derecho de suspender la ejecución de ejercicios subsiguientes en caso de existir facturas vencidas sin cancelar.
- No está incluido el costo de viáticos en caso tal de que la ejecución de actividades sea fuera de la ciudad de Bogotá.
- Plazo de pago: La factura debe ser cancelada dentro de los treinta (30) días calendario siguientes a la fecha de su radicación.
- Vigencia de la oferta: Sesenta (30) días calendario contados a partir de la fecha de recepción de la presente propuesta.

3.8 Limitaciones técnicas y exclusiones del servicio

No se incluye dentro de la prestación del servicio los siguientes puntos:

- Evaluación de seguridad física
- Pruebas de denegación de servicio a infraestructura o aplicaciones.
- Explotación de vulnerabilidades que supongan un riesgo para la operación de la organización.
- El alcance del servicio se limita exclusivamente a la ejecución de pruebas de hacking ético y análisis de vulnerabilidades, así como a la entrega de los informes correspondientes. No se incluye la implementación, ajuste, configuración, ni remediación de ningún tipo sobre la infraestructura tecnológica, aplicaciones, bases de datos, dispositivos de red u otros activos del cliente, independientemente de los hallazgos identificados.
- Generación de informes adicionales o diferentes a los pactados en la prestación del servicio.
- No se realizarán ajustes sobre el código de las aplicaciones.

- Las recomendaciones entregadas como resultado del servicio ofrecido no comprometen a A3Sec S.A.S. en forma alguna. La Entidad es responsable de validar la aplicabilidad de las recomendaciones entregadas y decidir sobre su implementación.
- A3Sec S.A.S. no será responsable por los efectos derivados de la no implementación de las recomendaciones entregadas, ni por decisiones del cliente que limiten o restrinjan el alcance del servicio. El cliente es responsable de validar la aplicabilidad de las recomendaciones y decidir sobre su implementación.

3.9 Condiciones generales para la prestación del servicio

Responsabilidades del cliente

- El cliente debe garantizar el acceso a los activos en el tiempo estipulado para las pruebas.
- Elaborar y firmar la carta de aprobación y permisos de realización de pruebas de análisis de vulnerabilidades, pentesting y Ethical Hacking.
- Proveer Información Relevante: El cliente deberá proporcionar toda la documentación necesaria sobre los sistemas, redes o aplicaciones que serán objeto de las pruebas, incluyendo configuraciones, arquitecturas y cualquier detalle técnico relevante.
- Notificar a Terceros Afectados: En caso de que las pruebas puedan afectar a terceros (usuarios, clientes, etc.), el cliente debe notificarles con antelación para evitar malentendidos o interrupciones en los servicios.

3.11 Servicios adicionales

Todo servicio, producto, actividad, requerimiento o cambio que no esté expresamente descrito en el alcance de la presente propuesta se considerará como un ítem adicional y, por tanto, no se encuentra incluido en el valor ofertado. La ejecución de cualquier ítem adicional deberá ser previamente solicitada y autorizada por escrito por el cliente, y estará sujeta a una cotización específica y

a su aceptación expresa. Ningún servicio adicional será ejecutado sin aprobación formal previa por parte del cliente. Se consideran servicios adicionales, entre otros: Evaluaciones técnicas adicionales no incluidas en el alcance original. Solicitudes de informes o entregables adicionales o en formatos distintos a los previstos. Solicitudes de ampliación del alcance durante la ejecución del servicio. Solicitud de retests fuera del plazo estipulado o en número superior al incluido en la propuesta. Cambios de infraestructura, activos o variables objeto de prueba, una vez iniciada la ejecución. Nos reservamos el derecho de rechazar o reprogramar la ejecución de actividades adicionales no contempladas en esta propuesta, hasta tanto no se haya aprobado formalmente su costo y condiciones por parte del cliente.

El inicio de los servicios descritos en esta oferta, se podrán programar de 1 a 2 semanas posteriores a la recepción de la Orden de Compra, firma del contrato y/o Aceptación de esta Propuesta firmada.

4. ACEPTACIÓN DEL PEDIDO

Términos y Condiciones

Las presentes condiciones rigen cualquier Orden de Compra (OC) de productos y servicios de A3Sec ("***Productos***") a la que se adjuntan, e incorporan por referencia las condiciones aplicables a cada Producto adquirido, indicadas en la Sección 4 más abajo.

1. Precio y Pago

Como contraprestación de los productos y servicios, que serán para el uso exclusivo del Cliente ("*not for resell*"), el Cliente se obliga a satisfacer a A3Sec el Precio Total según se especifica en la OC. Los importes establecidos en la OC (los "**Importes**") se indican y deben pagarse en dólares americanos y no incluyen ningún gasto adicional. Los cargos por manejo y envío son adicionales a los precios de Productos, a menos que se indique lo contrario expresamente en el momento de la venta. Los pagos realizados por el Cliente relacionados con este Acuerdo no son rembolsables. Salvo acuerdo contrario expreso en este Acuerdo, el Cliente realizará el pago dentro de 30 días naturales a partir de la fecha factura. La demora en el pago de dichos Importes devengará a favor de A3Sec intereses de demora y compensación de gastos de cobro, según ley aplicable, sin perjuicio de cualesquiera otros recursos o acciones de A3Sec frente a dicho incumplimiento. El pago se puede realizar por tarjeta de crédito, transferencia bancaria/electrónica, u otro método de pago previamente acordado.

A3Sec puede facturar parcialmente una OC. Las OC no aceptadas mediante su firma por A3Sec están sujetas a rechazo o cancelación por parte de A3Sec, bajo su única discreción. A3Sec no es responsable por los errores de precio, errores tipográficos u otros errores manifiestos en una propuesta u oferta de servicios, y se reserva el derecho de cancelar cualquier OC que resulte de dichos errores previa notificación al Cliente.

2. Impuestos

Los Importes no incluyen los Impuestos. El Cliente pagará a A3Sec una cantidad igual a los Impuestos que surjan o se relacionen con este Acuerdo, incluyendo, pero sin limitación, los derivados de ventas, servicios, uso o valor agregado, que son pagados o pagaderos por A3Sec. Los "***Impuestos***" incluyen cualquier forma de impuesto, gravamen, imposición, coste de aduana, recargo, contribución o arancel de cualquier naturaleza y impuesta por cualquier autoridad (incluyendo sin limitación cualquier multa, recargo o interés) sin incluir sin embargo, cualquier impuesto basado solamente en los ingresos neto de A3Sec. Si el Cliente debe, bajo cualquier ley o regulación aplicable, doméstica o extranjera, retener o deducir cualquier parte de los Importes pagaderos a A3Sec, entonces el importe que se debe pagar a A3Sec debe aumentarse por la cantidad necesaria para que A3Sec reciba una cantidad igual al importe que hubiera recibido si el Cliente no hubiera hecho retenciones o deducciones.

3. Integración y Envío

Los Productos serán integrados, configurados y enviados desde las instalaciones de A3Sec ubicadas en Colombia. La integración y configuración incluye la integración del software, hardware o servicio descrito en la oferta según las instrucciones del Cliente. Los términos de envío y propiedad INCO son ExWorks (EXW) para destinos en Colombia. Las fechas de envío son sólo estimaciones.

4. Confidencialidad y Publicidad

Ambas partes se comprometen a guardar secreto sobre los Productos y sobre cualquier hecho, noticia o dato del que tengan conocimiento en virtud de la conclusión, ejecución y/o resolución del presente Acuerdo, incluidos los precios y demás términos del mismo ("Información"). Las partes se comprometen a no divulgar esta Información confidencial, así como a no publicarla ni a hacerla pública en forma alguna, ni a ponerla a disposición de terceros, ya sea de forma directa o indirecta, sin el previo consentimiento escrito de la otra parte.

Durante el término de este Acuerdo, el Cliente y A3Sec puede participar en actividades de Co-marketing o publicidad, incluyendo anuncios comerciales, al establecerlo por escrito y aprobarlo. A3Sec también puede usar el nombre y logo del Cliente como referencia, en el sitio web de A3Sec, y en materiales de marketing. El Cliente acuerda servir como "referencia" para A3Sec, lo que significa que el Cliente puede recibir llamadas de parte de posibles clientes que busquen referencias, inversionistas potenciales o actuales, la prensa y analistas tecnológicos y financieros, por mutuo acuerdo de las partes.

5. Otras Condiciones

Este Acuerdo establece los términos y condiciones exclusivos con respecto la OC, sin integrar cualesquier términos diferentes o adicionales que puedan incluirse por parte del Cliente en el formulario de la OC u otro documento usado para enviar una solicitud de compra. Este Acuerdo representa la declaración final y completa

del acuerdo entre las partes, con respecto al asunto tratado y con respecto a todos los acuerdos previos escritos y acuerdos orales contemporáneos. Ninguna de las partes podrá ceder este Acuerdo ni cualquiera de los derechos u obligaciones dimanantes del mismo sin el consentimiento expreso de A3Sec, excepto que A3Sec podrá ceder libremente este Acuerdo a cualquier miembro de su grupo corporativo, o, en caso el supuesto de sucesión de empresas. Las condiciones aplicables a los Productos indicadas en la Sección 4 prevalecerán sobre estas condiciones de compra con respecto al uso o realización de los productos/servicios adquiridos. Si alguna parte de este Acuerdo no fuera ejecutable, total o parcialmente, dicha situación no afectará a la validez del resto del Acuerdo. Este Acuerdo de Compra tiene carácter mercantil, rigiéndose en lo no expresamente pactado en el mismo por las disposiciones del derecho mexicano. Las partes acuerdan expresamente someter cualquier conflicto o disputa derivada de este Acuerdo o su ejecución a los juzgados y tribunales de la ciudad de Bogotá, Colombia con expresa renuncia a su fuero propio, si fuera otro. No obstante, la validez, interpretación y aplicación de las Condiciones Generales aplicadas a los Productos y/o Servicios indicadas en la Sección 4 estarán gobernados por y constituidos de acuerdo con las leyes de Colombia, sin efecto de la Convención de las Naciones Unidas sobre Contratos para la Venta Internacional de Bienes. El Cliente por este medio irrevocablemente consiente a la jurisdicción exclusiva de los Tribunales en la ciudad de Bogotá. La fecha efectiva es la última fecha en que este Acuerdo fue firmado por ambas partes.

Los Productos y los datos técnicos y servicios relacionados (denominados colectivamente "Tecnología controlada") pueden estar sujetos a las leyes de importación y exportación de Colombia y/o a las leyes de cualquier país donde se importe o reexporte dicha Tecnología controlada. El Cliente acepta cumplir todas las leyes pertinentes y no exportar tecnología controlada contraviniendo dichas leyes ni a ningún país, entidad o persona prohibida para los que se necesite una licencia de exportación o cualquier otra aprobación gubernamental.

EN VIRTUD DE LO CUAL, cada parte ha firmado este Acuerdo, por sus representantes debidamente autorizados.

CLIENTE

_____
_____
Firma

A3Sec S.A de C.V.

Firma

_____
_____

Nombre _____ _____	Nombre
Puesto ----------	Puesto
Fecha ----------	Fecha

a3sec

‹BLINDAMOS ACTIVOS DIGITALES GLOBALMENTE›

‹ A3Sec España /›
C/ Aravaca,
6 2a Planta 28040
Madrid, España
T. +34 195330978

‹ A3Sec México /›
Río Lerma 232 Piso
23
Oficina 2325, Col.
Cuauhtémoc 06500
Ciudad de México
T. +52 55 8852 7975

‹ A3Sec Colombia
/›
Calle 98 #70-91
Oficina 913
Bogotá, Colombia
T.+57 1 2326863
+57 1 3099533