

ANEXO No. 2F ESPECIFICACIONES TÉCNICAS – SUSCRIPCIONES CAPTCHA

Las siguientes son las especificaciones técnicas mínimas que requiere la Entidad, para el cumplimiento del objeto contractual.

LAS ESPECIFICACIONES TÉCNICAS – FICHA TÉCNICA VAN DE ACUERDO CON LOS GRUPOS SEÑALADOS EN EL PLIEGO DE CONDICIONES.

GRUPO No. 6

DENOMINACIÓN TÉCNICA: ADQUISICIÓN DE SUSCRIPCIÓN PARA SERVICIOS DE CAPTCHA					
PLATAFORMA	CLASIFICACIÓN DEL BIEN O SERVICIOS	DESCRIPCIÓN	CANTIDAD	UNIDAD	VENCIMIENTO
CAPTCHA	43231513 o 43233205 o 81112501 o 81112202	Suscripción reCAPTCHA Empresarial - 200.000 assessments/mes	12	MES	N/A
	43231513 o 43233205 o 81112501 o 81112202	Suscripción reCAPTCHA Empresarial - 250.000 assessments/mes	12	MES	N/A
	43231513 o 43233205 o 81112501 o 81112202	Servicios de configuración, migración y transferencia de conocimiento	1	SERVICIOS	N/A
No.	OBLIGACIONES TÉCNICAS				
1.	Realizar la entrega e instalación de los servicios objeto del presente proceso, en el lugar señalado por el supervisor del contrato tanto para las plataforma y componentes requeridos, cuando se requiera.				
2.	DOCUMENTO DE DERECHO DE USO Y VIGENCIA: En el momento de la entrega de los elementos objeto del contrato, el contratista debe entregar documento donde se acredite el derecho de uso y vigencia para las suscripciones adquiridas				
3.	Realizar la activación del licenciamiento adquirido a partir de la suscripción del acta de inicio y en un término que no supere los 10 días hábiles				
4.	Realizar todos y cada uno de los informes solicitados por la supervisión del contrato.				
5.	El contratista deberá entregar al almacén de la Superintendencia de Industria y Comercio, las suscripciones de software requeridas en el presente proceso, cuando se requiera.				
6.	El oferente debe garantizar el acceso a consola de administración y métricas de seguridad				
7.	La herramienta debe permitir la integración con aplicaciones web (mínimo: Java, PHP, Angular, Javascript)				
8.	La herramienta debe permitir la integración con aplicación móvil (Android/iOS)				
9.	La herramienta debe permitir la detección y mitigación de bots y actividades fraudulentas en formularios y endpoints (incluida la señalización para decisiones de negocio ante intentos de apropiación de cuentas o abuso de credenciales).				
10.	La herramienta debe permitir Scoring/assessment por interacción y políticas por aplicación/formulario.				
11.	La herramienta debe bloquear eficazmente bots y scripts automatizados.				
12.	La herramienta debe resistir ataques de reconocimiento óptico de caracteres (OCR) y modelos de IA				
13.	La herramienta debe mitigar ataques como credential stuffing, brute force, scraping y DDoS con bots				
14.	La herramienta debe permitir el cifrado de las solicitudes y respuestas del CAPTCHA.				
15.	La herramienta debe garantizar la protección contra manipulación del código JavaScript para evitar bypass				
16.	La herramienta debe garantizar la imposibilidad de reutilizar tokens de CAPTCHA				
17.	La herramienta debe permitir validación segura del token del CAPTCHA en el backend antes de procesar solicitudes sensibles				
18.	La herramienta debe garantizar la protección contra ataques de replay, manipulación de parámetros o bypass por proxy.				
19.	La herramienta debe resistir ante ataques de clickjacking y CAPTCHA farming				
20.	La herramienta debe garantizar la protección frente a la interceptación de resolución mediante ataques Man in the Middle				
21.	La herramienta debe permitir el No almacenamiento de información sensible sin consentimiento del usuario				



Superintendencia de Industria y Comercio

22.	La herramienta debe garantizar el control sobre el intercambio de datos con terceros para evitar filtraciones
23.	La herramienta debe permitir la configuración de niveles de dificultad según el riesgo identificado
24.	La herramienta debe garantizar la integración con la arquitectura de seguridad existente
25.	La herramienta debe garantizar la capacidad de escalar sin afectar el rendimiento de la aplicación
26.	La herramienta debe cumplir con la normativa de la ley 1581
27.	La herramienta debe permitir una consola para visualización básica de eventos y métricas operativas del servicio
28.	El oferente debe entregar la documentación de la configuración (identificadores de propiedad, dominios autorizados, políticas de score y umbrales iniciales por formulario).
29.	El oferente debe entregar un reporte de puesta en marcha y entrega con evidencia de tráfico evaluado en producción
30.	Atender todas las solicitudes que hagan los supervisores, quienes informarán del funcionamiento defectuoso o la presencia de fallas en las suscripciones de software, las veces que sea necesario durante la vigencia
31.	La adquisición, renovación y/o actualización es por la vigencia de un (1) año, a partir de la instalación de las suscripciones requeridas en el proceso de contratación, lo cual no debe superar cinco (5) días calendario desde la suscripción del acta de inicio.
32.	Efectuar la entrega de la documentación técnica de los bienes adquiridos al personal (técnico y funcional) de la SIC encargado de su funcionamiento y custodia, en caso de requerirse
33.	La suscripción debe tener soporte 8x5 de un (1) año por el fabricante, incluida actualizaciones del software durante el tiempo de suscripción.
34.	El oferente debe suministrar el protocolo de escalamiento y ANS para la gestión de los requerimientos de servicios
35.	El oferente debe garantizar que los servicios se presten como mínimo para: Assessment, diseño, parametrización, migración desde versión gratuita y estabilización, sin afectar el código fuente de los sistemas de información que deban intervenir
36.	La activación y estabilización del servicio se realizará en un periodo corto y la aprobación de la Entidad, que no debe superar dos (2) semanas
37.	El Contratista debe suministrar mínimo 4 horas de transferencia de conocimiento, dentro de la cual se traten temas de instalación, configuración y nuevas funcionalidades de la solución para la SIC.


Adriana Cetina Hernández
Jefe Oficina de Tecnología e Informática

Proyectó: Ricardo Delgado Montes – Contratista Jefatura OTI 
Revisó: Magda Julieth Zarrate Saldaña – Coordinador G. de Trabajo de Informática Forense y Seguridad Digital 
Diana Marcela Gualteros Sanchez - Abogada Jefatura OTI 
Nelson Romero Muñoz– Contratista Jefatura OTI 
Mauricio Salgado Guzman – Contratista GST OTI 
Demys Alberto Díaz Aparicio – Coordinador G. de Trabajo de Servicios Tecnológicos 
Aprobó: Adriana Cetina Hernández – Jefe OTI 

