Corpocaldas
Corporación Autónoma Regional de Caldas

CORPORACIÓN AUTÓNOMA REGIONAL DE CALDAS
INVITACIÓN A PRESENTAR PROPUESTA
CONTRATACIÓN DIRECTA TRC-2024-0241
Servicio de infraestructura, actualización, mantenimiento e innovación de la página web de la Corporación.

Manizales, agosto 26 de 2024

Señores
ALTIC
COLOMBIA

REFERENCIA: Invitación a presentar propuesta

Respetado Señores ALTIC CONSULTING:

LA CORPORACIÓN AUTÓNOMA REGIONAL DE CALDAS se encuentra interesada en recibir oferta para celebrar el contrato de prestación de servicios único oferente conforme a los siguientes términos:

1. OBJETO

Servicio de infraestructura, actualización, mantenimiento e innovación de la página web de la Corporación.

2. OBLIGACIONES GENERALES

- Ejecutar el contrato de conformidad con lo establecido en los estudios previos, la propuesta aceptada y el contrato.
- Suscribir oportunamente el acta de inicio y el acta de liquidación del contrato, conjuntamente con el supervisor del mismo, cuando corresponda.
- Entregar al supervisor informe de las actividades ejecutadas de conformidad con la periodicidad dispuesta en los documentos que forman parte integral del presente contrato.
- Mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del contrato, así como, respetar la titularidad de los derechos de autor, en relación con los documentos, obras, creaciones que se desarrollen en ejecución del contrato, en caso que aplique.
- Cumplir con el objeto del Contrato con plena autonomía bajo su propia responsabilidad y por lo tanto, sin que exista ningún tipo de subordinación, ni vínculo laboral alguno entre las partes.
- Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y en trabamientos de cualquier índole.
- Utilizar de manera racional los recursos energéticos e hídricos de las instalaciones donde ejecuta sus actividades; así mismo realizar uso eficiente de los materiales e insumos; efectuar el manejo y disposición adecuada de los residuos sólidos ordinarios, peligrosos, especiales, igualmente realizar control y tratamiento de vertimientos y emisiones atmosféricas que se generen en ejercicio de las actividades derivadas de la ejecución del contrato.

- Entregar para cada pago, la certificación suscrita por el representante legal o revisor fiscal, que acredite el cumplimiento del pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar de los últimos seis (6) meses, de conformidad con el artículo 50 de la Ley 789 de 2002 o aquella que lo modifique, adicione o complemente.
- Responder por sus actuaciones y omisiones derivadas de la celebración y ejecución del Contrato.
- Cancelar los impuestos tasas, y contribuciones aplicables al contrato, dada su naturaleza y cuantía, por lo cual autoriza expresamente a CORPOCALDAS para que de ser necesario descuente los valores correspondientes a dichas obligaciones.
- Desarrollar con diligencia las actividades objeto del Contrato.
- Comunicar al supervisor los asuntos que surjan en desarrollo del Contrato y que puedan alterar el normal desarrollo del mismo. Esto incluye cualquier noticia que tenga sobre la posible comisión de delitos y/o la afectación de derechos humanos o que afecten el medio ambiente.
- Cumplir con las políticas sobre prevención y control del lavado de activos, financiación del terrorismo y otras actividades delictivas.
- Utilizar en la prestación de los servicios el Manual de Identidad Corporativa de CORPOCALDAS.
- Las demás inherentes a la naturaleza del Contrato

3. OBLIGACIONES ESPECIFICAS

- Realizar el soporte y mantenimiento a la infraestructura tecnológica que soporta la operación de las plataformas de la entidad relacionadas con Gobierno Digital, incluyendo el servidor principal, el servidor secundario, los certificados digitales de la corporación, los servicios de visualización de Datos de Inteligencia de Negocios, así como los servicios relacionados con Accesibilidad, Bolsa de emails (10000 mensuales) y SMS (2000 mensuales).
- Renovación certificado digital SSL de tipo wildcard, que pueda ser utilizado por el sitio web de la Corporación o de cualquiera de sus subdominios en cualquier servidor, como parte del despliegue de su infraestructura cloud, apoyar en el despliegue del mismo cuando sea necesario.
- Integrar, configurar y entrenar servicio de chat con la página web de la corporación que cuente con la capacidad de crear una base de conocimiento para dar respuesta a preguntas frecuentes y automatización de las mismas a través del ChatBot.
- Utilizar los componentes de accesibilidad presentes en la página actual de la Corporación por la vigencia del contrato.
- Proveer un servidor exclusivo para soportar páginas desarrolladas en WordPress para la Corporación entre ellos el de fotografía ambiental, el grupo de investigación y el de negocios verdes.
- Prestar soporte a la aplicación móvil de Corpocaldas dentro de los store de Android y IOS.
- Soporte a usuario técnico o de la oficina TIC de la entidad.
- Realizar mantenimientos correctivos y preventivos a la plataforma de Gobierno Digital.

- Componente de seguridad avanzado para protección del sitio web de la corporación ante ataques cibernéticos, mediante el monitoreo continuo, configuración y habilitación de firewall dedicado de seguridad, escaneo y remoción de malware, atención prioritaria en caso de catástrofes y acompañamiento de personal experto en seguridad.
- Realizar copia de seguridad de contenido, bases de datos, imágenes, documentos, archivos multimedia, scripts, entre otros de la página web, diaria.
- Realizar 1 copia de seguridad espejo del servidor total que contiene la página web 1 vez a la semana.

4. PRESUPUESTO OFICIAL

El valor máximo del contrato es de Treinta millones novecientos dieciséis mil doscientos pesos mcte ($30.916.200) (exento de IVA)

PROPUESTA

Fecha límite de entrega de la propuesta:	27 de Agosto de 2024
Hora:	4:00 p.m.
Lugar de entrega:	Piso 22 Corpocaldas
Correo:	rubenjaramillo@corpocaldas.gov.co

DOCUMENTOS DE LA PROPUESTA

Los interesados en participar deben cumplir los siguientes requisitos:

a.) - CERTIFICADO DE EXISTENCIA Y REPRESENTACION (MAX 2 MESES)
b.) - COPIA CÉDULA RTE LEGAL
c.) - AUTORIZACIÓN PARA RTE LEGAL (CUANDO APLIQUE)
d.) - ANTECEDENTES DISCIPLINARIOS PROCURADURIA RTE LEGAL
e.) - ANTECEDENTES DISCIPLINARIOS PROCURADURIA PERSONA JURÍDICA
f.) - ANTECEDENTES FISCALES CONTRALORIA RTE LEGAL
g.) - ANTECEDENTES FISCALES CONTRALORIA PERSONA JURIDICA
h.) - CONSULTA DE ANTECEDENTES PENALES Y REQUERIMIENTOS JUDICIALES RTE LEGAL
i.) - CONSULTA DEL REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS. RTE LEGAL
j.) - PAZ Y SALVO PARAFISCALES
k.) - TARJETA PROFESIONAL REVISOR FISCAL (CUANDO APLIQUE)
l.) - ANTECEDENTES DISCIPLINARIOS DEL REVISOR FISCAL (CUANDO APLIQUE)
m.) – RUT

5. PLAZO

6 meses contados a partir del cumplimiento de los requisitos de perfeccionamiento, legalización y ejecución del contrato.

6. FORMA DE PAGO

CORPOCALDAS cancelará el valor del contrato previa presentación de la factura correspondiente y autorización de pago por parte del supervisor, en la que se verifique el cumplimiento del objeto contratado y el pago de seguridad social integral y A.R.L de la siguiente manera:
6 pagos mensuales, correspondientes al servicio de mantenimiento, actualización y soporte técnico por valor de $5.152.700 cada uno.

Cordialmente,

Rubén Darío Jaramillo Parra
Profesional Especializado – TIC
Corpocaldas

Manizales, agosto 27 de 2024

Señores
CORPORACIÓN AUTÓNOMA REGIONAL DE CALDAS
CORPOCALDAS
ATT: Rubén Darío Jaramillo Parra

REF: Descripción Alcance del Servicio de Soporte Actualización, Mantenimiento – SAM para la Plataforma de Servicios Tecnológicos de Gobierno Digital para CORPOCALDAS

Nos permitimos presentar la descripción de la propuesta de servicios relacionados con el Soporte, Actualización, Mantenimiento de la plataforma de servicios tecnológicos basada en la nube para la configuración, administración, integración, comunicación y planeación para la Corporación Autónoma Regional de Caldas, cumpliendo con los lineamientos contemplados en la política de gobierno digital de la República de Colombia, de acuerdo con las características técnicas y funcionales que se detallan a continuación:

Características Técnicas

La presente propuesta de servicios contempla 3 componentes fundamentales para el correcto funcionamiento de la actual plataforma tecnológica que soporta los procesos de Gobierno Digital en la Corporación, buscando en primera instancia continuar con el cumplimiento de la reglamentación exigida por el Gobierno Nacional a través de los decretos 1078 de 2015 y 1008 de 2018 los cuales reglamentan los lineamientos y las políticas de la estrategia de Gobierno Digital en Colombia, sino que también pretende asegurar la evolución y el mejoramiento continuo de los sistemas de información, la infraestructura tecnológica, el modelo de servicio y la ampliación de los canales de

comunicación con los ciudadanos. Para ello se plantea los siguientes componentes de intervención:

1. Infraestructura Tecnológica

Este primer componente incluye todos los servicios de la infraestructura tecnológica que soporta la operación de las plataformas de la entidad relacionadas con Gobierno Digital, incluyendo el servidor principal, el servidor secundario, los certificados digitales de la corporación, los servicios de visualización de Datos de Inteligencia de Negocios, así como los servicios relacionados con Accesibilidad, Bolsa de emails y SMS cumpliendo con las siguientes características:

ITEM	*ESPECIFICACIONES*
Infraestructura	
Tamaño de la Instancia	D4: SSD, 8 cores, 64 GB RAM, 960GB SSD, y 2TB SATA con posibilidad de escalabilidad El uso actual del SSD es del 45% y el del SATA es del 10%, se realiza un sobredimensionamiento de la infraestructura actual para soportar posibles controles de cambios, crecimiento de la base de datos o requerimientos futuros que requieran crecer los parámetros de almacenamiento.
Máquinas Virtuales	(SQL Server 2019 bajo 64-bit - ASP.NET Framework 4.5, Windows Server 2022, Microsoft IIS (internet Information Services) 10 o superior.
Firewall	Firewall que se gestione directamente con la administración de los endpoints, tanto bases de datos como para los front de cada aplicación web.
Tecnología	Por compatibilidad con la infraestructura de la Corporación, la plataforma de gobierno digital debe estar soportar sobre SQL Server como motor de base de datos y .Net C# como lenguaje de programación.
Cloud Hosting	
Almacenamiento	Objetos binarios grandes que proporcionan colas para la comunicación entre componentes. Implementación de Blob Storage para almacenamiento de archivos. El almacenamiento podrá tener un crecimiento adicional del 50% del espacio actualmente asignado sin costo adicional y haciendo uso del Blob Storage.
Servicios de Infraestructura	Posibilidad de desplegar de una forma sencilla máquinas virtuales.

Ubicación de Infraestructura	Los servidores deben estar alojados en centros de datos con altas medidas de seguridad para impedir que personas fio autorizadas puedan acceder físicamente a ellas o perturbar su funcionamiento
Certificado Digital – SSL	Se deberá entregar configurado e instalado un certificado digital – SSL de tipo Wildcard, que pueda ser utilizado por el sitio web de la Corporación o de cualquiera de sus subdominios como parte del despliegue de su infraestructura cloud. ALTIC proporcionará de igual manera un certificado SSL tipo Wildcard para UN Servidor On-Premise dentro de la infraestructura de la Corporación.
Email / SMS	
Paquete de Correos Electrónicos	Envío de hasta 10.000 correos electrónicos mensuales.
SMS	Envío de hasta 2.000 SMS mensuales.
Visor de Business Intelligence	
Licencia de PowerBI Desktop	Se incluye una licencia de PowerBI Desktop, para el desarrollo de tableros BI para los diferentes procesos relacionados con la política de Gobierno Digital. La Publicación se realizará desde el mismo servicio de PowerBI, mediante el uso de su plataforma de publicación de información pública. Se apoyará a la Corporación hasta con 90 horas para el montaje de seis nuevos dashboards los cuales deberán ser definidos por la entidad.
Servicios Adicionales	
Accesibilidad	Renovación de licencia de la herramienta para accesibilidad para sitios web públicos la cual permite el cumplimiento de la normativa de accesibilidad WCAG 2.1 AA, ADA, Sección 508 – Se entrega por un Período de un año.
Licencia de Chat	Licenciamiento de Plataforma de Chat personalizado y con plena integración al sitio web de CORPOCALDAS, incluye: completa personalización de entrono de Chat y Live Chat para usuarios.

Servidor WordPress	Para proteger la integridad de la infraestructura principal que soporta la plataforma DIGITALGOB, se provee un servidor exclusivo para soportar páginas desarrolladas en WordPress para la Corporación y de esta forma proteger la infraestructura CLOUD donde se alojan los sitios y los servicios principales. Igualmente, dentro de la propuesta se cubre la renovación de 3 dominios .COM, los cuales son utilizados para el concurso de fotografía, el plan de acción y negocios verdes se listan a continuación: fotografiaambiental.com negociosverdescorpocaldas.com plandeaccioncorpocaldas.com Cabe aclarar que el dominio de la Corporación (GOV.CO) no presenta vencimiento por lo cual no requiere ser renovado y que cubre la creación de los subdominios que sean requeridos sin costo adicional.

La presente propuesta cubre la actualización / renovación de los siguientes servicios hasta la fecha estimada de renovación que se lista a continuación:

Nombre del Servicio	**Fecha Vencimiento 2024**	**Fecha Estimada Renovación 2025**
Negocios Verdes negociosverdescorpocaldas.com Dominio	2024-08-29	2025-08-29
Plan de Acción plandeaccioncorpocaldas.com Dominio	2025-04-11	2025-04-11
Fotografía Ambiental fotografiaambiental.com Dominio	2024-09-30	2025-09-30
Hosting Servicios WordPress Business WordPress Infraestructura Cloud	2024-10-05	2025-10-05
Wild Card SSL Infraestructura Cloud	2024-12-27	2025-12-27
Wild Card SSL Infraestructura ON-Premise	2025-04-29	2025-04-29
Licencia PowerBI Desktop Dashboard PowerBI	2024-09-30	2025-09-30

Licencia UserWay Componente de Accesibilidad	2024-09-30	2025-09-30
Licencia Chat LiveChat	2024-08-31	2025-08-31

Los demás servicios tienen un ciclo de renovación mensual y se asegura su funcionamiento hasta el 2025-02-28 a excepción del servicio de Infraestructura Cloud que soporta la página web y de servicios de la Corporación y este se extiende hasta máximo el 2025-03-31

2. Soporte Actualización, Mantenimiento

Al ser **DIGITALGOB** una plataforma como servicio, este componente extiende, por el período de vigencia del contrato, la resolución de las solicitudes de soportes a usuario técnico o del área de sistemas de la entidad relacionadas con las funcionalidades contempladas en el alcance inicial planteado en el contrato número 238-2020, así como la inclusión de aquellos mantenimientos correctivos y preventivos que se realicen durante este período de tiempo a la plataforma de Gobierno Digital.

La presente propuesta NO incluye el desarrollo de solicitudes de que involucre actividades de desarrollo de nuevas funcionalidades o que involucre un componente de innovación.

Dentro del alcance de mantenimiento incluyen los siguientes componentes:

- Funcionalidad de Texto en Audio, se activa mediante el componente de Accesibilidad de UserWay y se activa por un año.
- Inclusión de la opción de Centro de Relevo.

3. Componente de Protección y Seguridad para el Sitio Web

Componente de seguridad avanzado para protección del sitio web de la Corporación ante ataques cibernéticos, mediante el monitoreo continuo, configuración y habilitación de firewall dedicado de seguridad, escaneo y remoción de malware, atención prioritaria en caso de catástrofes y acompañamiento de personal experto en seguridad, permitiendo mejorar la seguridad actual del sitio web de la Corporación a través de los siguientes componentes:

- Protección de Sitio Web
- Malware y remoción de hackeos por expertos en seguridad
- 12 de horas de restablecimiento de servicios ante catástrofe
- Reporte detallado después de cada evento de limpieza y recuperación
- Escaneo y monitoreo de seguridad cada 6 horas
- Firewall a nivel de Aplicación WEB – WAF
- Monitoreo y remoción de listas negras y listas
- Monitoreo y soporte de SSL
- Detención de Hackeos – Virtual Patching / Hardening
- Protección de Firewall – HTTPS & Cumplimiento PCI
- Mitigación avanzada en DDoS
- Mejora de velocidad de respuesta CDN
- Balanceo de carga / Alta disponibilidad

Este componente es uno de los más importantes dado el creciente número de ataques que los sitios web de entidad estatales y gubernamentales han venido sufriendo recientemente, de acuerdo con el informe presentado por la Cámara Colombiana de Informática y Telecomunicaciones en su informe de abril de 2022, a esa fecha más de "…193 sitios web de entidades públicas colombianas, han sido infectados y se han

sustraído datos de usuarios gubernamentales o de servicios públicos con el fin de distribuirlos y venderlos en la Deep web…" Lo que nos lleva a incluir de forma inmediata dentro del esquema de configuración y seguridad para el sitio web de Corpocaldas.

También se deben considerar los siguientes lineamientos para el cumplimiento del componente de seguridad en Corpocaldas y que se relacionan con la Resolución 1519 de 2020 del MinTIC donde se establecen las Condiciones mínimas técnicas y de seguridad digital:

CONDICIONES DE SEGURIDAD DIGITAL
Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software
Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones
Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).
Aplicar mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.
Proteger la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos; (iii) la sanitización y escape de variables en el código; (iv) verificación estándar de las Políticas de Origen de las cabeceras; y (v) la verificación y comprobación del token de CSRF (cuando aplique).
Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios.
Exigir mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y solicitar renovaciones periódicas de las mismas garantizando la accesibilidad de persona con discapacidad.
Mantener actualizado el software, frameworks y plugins de los sitios web.
Restringir el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.
Ocultar y restringir páginas de acceso administrativo.

Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.
Crear copias de respaldo.
Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.
Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones. (adicional al cifrado SSL), También deben habilitar las cabeceras de seguridad, entre otras las siguientes: Content-Security-Policy (CSP), X-Content-Type- Options, X-Frame-Options, X-XSS-Protection, Strict-Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature-Policy.
Implementar mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas, incluyendo la accesibilidad para las personas con discapacidad.
Proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación.
Sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script», además de la restricción de formatos y tamaños para subida de archivos.
Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación)
Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Project (OWASP).
Implementar en los servidores los controles necesarios (hardware o software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.
Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.
Implementar monitoreos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes.
Establecer los planes de contingencia, DRP y BCP, que permita garantizar la continuidad de la sede electrónica o del sitio web 7/24 los 365 días del año.
Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.
Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos de este.
Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.

PROGRAMACIÓN DEL CÓDIGO FUENTE
Los sujetos obligados, en todos sus sitios web, móvil y aplicaciones deberán implementar estándares de desarrollo seguro para evitar vulnerabilidades el código fuente y errores de presentación o alteraciones en el contenido de la información dispuesta al público. Así mismo, se deben evitar mecanismos que puedan poner en riesgo la información o los datos personales o sensibles.
Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones.
Cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C (World Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios.
Adoptar validadores HTML y CCS para la continua revisión del sitio web y su mejora continua, a través de las buenas prácticas del W3C (World Web Wide Consortium).
Cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO, incluyendo la validación de la codificación, en caso de que les aplique.
Incluir lenguaje común de intercambio para la generación y divulgación de la información y datos estructurados y no estructurados dispuestos en medios electrónicos, como los sitios web de los sujetos obligados y el Portal Único del Estado Colombiano GOV.CO, en caso de que les aplique.
Implementar un sistema de control de versiones (Git), que permitan planear y controlar la vida de la aplicación, y en una fase a mediano plazo poder implementar un sistema de integración, cambio y despliegue continuo.

Presupuesto:

La presente propuesta tiene un valor total de **$30.916.200 y está exento de IVA**.

Cubre los servicios descritos en los numerales anteriores por 6 meses hasta el 28 de febrero del año 2025.

A continuación, presentamos un cuadro detalle con el valor de cada componente de forma individual para su conocimiento:

Componente	Valor
Infraestructura Incluye todos los componentes descritos en el numeral 1 de la presente propuesta incluido el servidor, certificados digitales, renovación de dominios, licencias de chat, paquete de accesibilidad, bolsa de emails y SMS, servicios de WordPress, licencias de PowerBI Desktop para la entidad	$22.656.900
Soporte, Actualización, Mantenimiento Incluye todas aquellas actividades relacionadas con el proceso de SAM durante la vigencia del contrato, incluyendo las tareas de mantenimiento correctivo y preventivo de la plataforma DIGITALGOB	Incluido en Precio como valor agregado
Componente de Seguridad y Protección para el Sitio Web Incluye todos los componentes descritos en el numeral 4 de la presente propuesta, destacando: Firewall, Monitoreo de vulnerabilidades, Limpieza de Malware y Hacks, asistencia prioritaria en caso de ataque, monitoreo de listas negras, **cumplimiento de la Resolución 1519 de 2020, entre otras características.**	$8.259.300
TOTAL	**$30.916.200**

Quedamos atentos ante cualquier inquietud o ampliación de información que puedan necesitar.

Cordialmente,

OSCAR CUESTA MEZA
ALTIC Consulting SAS

Manizales, agosto de 2024

REFERENCIA: Prestación de servicios Persona Jurídica Único Oferente

OBJETO: Servicio de infraestructura, soporte, actualización, mantenimiento de la página web de la corporación.

ASUNTO: **Certificación de idoneidad**

En los estudios previos se estableció el siguiente requisito.

Persona Jurídica que tenga el derecho de explotación exclusiva de la plataforma tecnológica GOBTIC, herramienta tecnológica para el montaje, desarrollo y ejecución de la política de Gobierno Digital en organizaciones públicas del orden estatal, departamental y municipal.

Acreditación del requisito

Para la celebración del contrato se solicitó a la empresa Altic Consulting el certificado de derechos de autor, allego certificado del ministerio del interior con los siguientes datos:

- Libro-Tomo-Partida: 13-70-384
- Fecha de registro: 13 de diciembre de 2018
- Datos de la obra: GOBTIC

De conformidad con lo expuesto, se certifica la idoneidad de la empresa para continuar con el proceso de contratación de conformidad con lo establecido en los estudios previos.

EVALUADOR

RUBEN DARIO JARAMILL PARRA
PROFESIONAL ESPECIALIZADO

CÉSAR AUGUSTO CANO CARVAJAL
SUBDRIRECTOR ADMINISTRATIVO Y FINACIERO