RESOLUCIÓN No. 029 DE 2022
ENERO 25 DE 2022

"Por medio de la cual se declara procedente el uso de la modalidad de contratación directa en un proceso de contratación pública"

LA GERENTE DEL FONDO DE BIENESTAR SOCIAL DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

En ejercicio de sus atribuciones legales y en especial de las conferidas por el Artículo 30 de la Ley 80 de 1993 y la Ley 1150 de 2007.

CONSIDERANDO:

Que el Artículo 2.2.1.2.1.4.1° del Decreto 1082 de 2015, establece que salvo en los casos en que el contrato a celebrar sea de prestación de servicios profesionales y de apoyo a la gestión:

"(…) la Entidad Estatal debe señalar en un acto administrativo la justificación para contratar bajo la modalidad de contratación directa, el cual debe contener:

1. *La causal que invoca para contratar directamente.*

2. *El objeto del contrato.*

3. *El presupuesto para la contratación y las condiciones que exigirá al contratista.*

4. *El lugar en el cual los interesados pueden consultar los estudios y documentos previos."*.

Que, el Literal g), Numeral 4° del Artículo 2° de la Ley 1150 de 2007, establece que es causal de contratación directa "c*uando no exista pluralidad de oferentes en el mercado".*

Que, el Decreto 1082 de 2015. en su Artículo 2.2.1.2.1.4.8°, reglamentó lo anterior, estableciendo que no existe pluralidad de oferentes en el mercado, *"cuando existe solamente una persona que puede proveer el bien o el servicio por ser titular de los derechos de propiedad industrial o de los derechos de autor, o por ser proveedor exclusivo en el territorio nacional".*

Que, el objeto de la contratación consiste en *"Adelantar el mantenimiento del software portal institucional".*

Que para efectos de realizar la precitada contratación se cuenta con un presupuesto de OCHENTA Y CINCO MILLONES NOVECIENTOS CUARENTA Y UN MIL PESOS MTCE ($ 85.941.000) respaldado con el CDP 2122 del 18 de enero de 2022, afectando el Rubro A-03-04-02-016 SERVICIOS MÉDICOS, EDUCATIVOS, RECREATIVOS, Y CULTURALES, expedido por el responsable del Área de Presupuesto de la Entidad.

Que el Fondo de Bienestar Social de la Contraloría General de la República, como parte de la implementación del manual de Gobierno digital en su componente de información, ha adelantado el desarrollo y puesta en publicación del portal institucional de la entidad a través del dominio www.fbscgr.gov.co. Con el fin de dar cumplimiento al decreto 2693 de 2012 y al manual de Gobierno en línea.

Que el portal institucional no se alberga dentro del DATACENTER de la entidad, por lo cual se encuentra tercerizado para asegurar una disponibilidad del 99.6%, de igual manera minimizar los posibles ataques a los sistemas de la entidad toda vez que las direcciones IP del dominio no se encuentran publicadas

por lo cual no son fáciles de detectar, de igual manera mantener un esquema de seguridad conforme a la norma ISO 27000 y sus sub-series. Como herramienta de visualización y presentación de información, el portal institucional se ha ajustado a un esquema más ágil y armonizado conforme a los estándares de la entidad. En cuanto a participación ciudadana se habilitaron salas de chat, interacción mediante PQRS, correos de notificaciones, subsitios destinados al Centro Médico, Colegio de la CGR y portal de niños.

Que en la actualidad, en desarrollo de las actividades de implementación de la política de gobierno digital, es necesario adelantar el mantenimiento del portal institucional.

Que el administrador de contenidos CMS, es propiedad intelectual de la empresa MICROSITIOS, por lo tanto, el Fondo de Bienestar Social de la CGR, cuenta con su licencia de uso, más no de modificación, de igual manera es necesario contar con personal con conocimientos específicos en programación PHP y en el CMS de MICROSITIOS.

Que es necesario realizar el mantenimiento de las rutinas programadas en el portal institucional con el fin de optimizar el acceso al mismo con la reducción en los tiempos de ejecución de las rutinas que componen el código del mismo, también es requerido hacer la depuración de la información obsoleta almacenada en el portal institucional.

Que se debe continuar con apertura a la accesibilidad de la información a través del portal institucional mediante el uso de los foros y chats que se encuentran configurados en el portal, de igual manera es necesario continuar con el ajuste de la APP de FBSCGR para aumentar la masificación de su uso y presentar la información en dispositivos móviles de fácil uso y alcance.

Que con el fin de darle cumplimiento a la resolución 2710 del 7 de octubre de 2017 del MINTIC "en la cual se establecen los lineamientos para la adopción del protocolo IPV6" el portal del Fondo de Bienestar Social de la CGR, el portal requiere de mantenimiento para asegurar la conectividad en este direccionamiento.

Que para cumplir con lo solicitado en la Directiva 03 de 2019 y en el Decreto 2106 de 2019 es necesario el rediseño del portal institucional a fin de ajustarlo a los estándares solicitados en la normatividad vigente, por esta razón se requiere del rediseño gráfico del portal y la implementación de la sede electrónica del FBSCGR.

Que según certificado de registro de soporte lógico del Ministerio del Interior y Justicia de la unidad de Derechos de Autor Libro 13 tomo 13 partida 348, y fecha de registro 19 de enero de 2005, aparece registrado a nombre de la empresa MICROSITIOS S.A.S., la obra ADMINISTRADOR DE CONTENIDOS – MICROSITIOS CONTENT MANAGER, este administrador de contenidos es la base del portal institucional del Fondo de Bienestar Social de la CGR, razón por la cual es la única persona jurídica que puede proveer el ya referido servicio.

Que de la necesidad planteada y de las circunstancias descritas anteriormente quedó constancia en el estudio previo que soporta la contratación, el cual fue proyectado por el Profesional Especializado Grado 14 del Área de Sistemas y se encuentra firmado por el Director Administrativo y Financiero del Fondo de Bienestar Social de la Contraloría General de la República.

Que, de conformidad con lo señalado en los numerales 2.6, 2.7, 2.8 y 8.1 del referido estudio previo, el Fondo de Bienestar Social de la Contraloría General de la República exigirá al contratista para la ejecución del objeto contratado las siguientes condiciones:

*"**2.6 Especificaciones técnicas:***

1. IMPLEMENTACION RESOLUCION 1519 DE 2020 ANEXOS 1, 2 y 3:
1.1 Ajustes al Diseño gráfico y modificación de menús
1.2 Implementación del ANEXO 1 – Directrices de Usabilidad web:
- *1.2.1 Subtítulos, Closed Caption y Alternativa texto para elementos no textuales*
- *1.2.2 Implementación del mapa del sitio en XML*
- *1.2.3 Implementación del mapa del sitio*
- *1.2.4 Permanencia e integralidad de accesibilidad en versión responsive*
- *1.2.5 Lenguaje de marcado bien utilizado*
- *1.2.6 Etiqueta canónica*

1.2.7 Orden de tabulación adecuado de los contenidos y visualización del foco
1.2.8 Advertencias bien ubicadas
1.2.9 No utilizar audio automático
1.2.10 Permitir control de contenidos con movimiento y parpadeo
1.2.11 No generar actualización automática de páginas
1.2.12 Integralidad de la accesibilidad
1.2.13 No generar cambios automáticos al recibir el foco o entradas
1.2.14 Ajuste de formularios
1.2.15 Enlaces adecuados
1.2.16 Idioma
1.2.17 Imágenes de texto
1.2.18 Codificación UTF-8
1.2.19 Páginas y formularios manejables por teclado
1.2.20 Lenguaje de marcado accesible
1.2.21 Buen uso de tablas y listas
1.2.22 Plantillas accesibles

1.3 Implementación del ANEXO 3 - Condiciones mínimas técnicas y de seguridad digital:

1.3.1 [DESARROLLO] Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software
1.3.2 [DESARROLLO] Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones
1.3.3 [INFRAESTRUCTURA] Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).
1.3.4 configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.
1.3.5 [DESARROLLO] 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
(v) la verificación y comprobación del token de CSRF (cuando aplique).

1.3.6 [INFRAESTRUCTURA] 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.
1.3.7 [DESARROLLO] 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.
1.3.8 [INFRAESTRUCTURA] Mantener actualizado el software, frameworks y plugins de los sitios web.
1.3.9 [DESARROLLO] 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.
1.3.10 [DESARROLLO] Ocultar y restringir páginas de acceso administrativo.
1.3.11 [INFRAESTRUCTURA] Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.
1.3.12 [INFRAESTRUCTURA] Crear copias de respaldo.
1.3.13 [INFRAESTRUCTURA] Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.
1.3.14 [INFRAESTRUCTURA] Garantizar conexiones seguras a través del 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.
1.3.15 [INFRAESTRUCTURA Y DESARROLLO] 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.
1.3.16 [INFRAESTRUCTURA] 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.
1.3.17 [DESARROLLO] 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.
1.3.18 [DESARROLLO] Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación)
1.3.19 [INFRAESTRUCTURA] 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).
1.3.20 [INFRAESTRUCTURA] 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.
1.3.21 [DESARROLLO] Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.

1.3.22 [INFRAESTRUCTURA] 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.

1.3.23 [INFRAESTRUCTURA] 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.

1.3.24 [INFRAESTRUCTURA] Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.

1.3.25 [INFRAESTRUCTURA] Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos del mismo.

1.3.26 [INFRAESTRUCTURA] Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web

2. *MANTENIMIENTO Y SOPORTE REMOTO PORTAL WEB y APP:*

   Se ofrece el servicio de revisión y actualizaciones para el portal de la entidad y comprende todas aquellas actividades que buscan mejorar el portal actual o la prestación del servicio. Las actividades ofrecidas son:
   Capacitaciones de manejo del CMS a funcionarios de la entidad cuando lo soliciten
   Instalación del certificado de seguridad SSL del portal web
   Actualizaciones de Seguridad al CMS actual de la Entidad
   Compactación y optimización de la base de datos.
   Mejoras gráficas menores, botones, cambio de colores etc. Verificación de espacio en el disco duro
   Verificación del uso de memoria por las diferentes aplicaciones
   Revisión de los logs del sistema
   Compactación y reparación de tablas defectuosas
   Monitoreo remoto
   Cuarenta (40) horas de desarrollo en PHP de funcionalidades a la medida, Diseños a la medida y cambios estructurales del portal.

3. *Suministro del Hosting del portal institucional, Se deben asegurar las siguientes condiciones técnicas:*

- *Modalidad: Cloud IaaS*
- *Procesadores: 4 CPUs*
- *Memoria RAM: Hasta 16 GB*
- *Espacio en disco: Hasta 500GB*
- *Transferencia: Hasta 4Tb/mes*
- *Ubicación del DATACENTER de Nueva York, con posibilidad de otras regiones.*
- *Imágenes de disco: respaldo semanal automático (imagen idéntica del servidor)*
- *Backups: copia diaria completa de la base de datos y una copia diaria diferencial de los archivos publicados en el portal*
- *Dirección IP flotante*
- *Soporte IPv6-IPv4.*
- *Certificado SSL.*
- *Software base: Linux CentOS 8.2 x64 / Debian 9 x64 Apache 2.4 en su última versión estable disponible*
- *PHP 7.2 en su última versión disponible*
- *MySQL / MariaDB*
- *Monitoreo interno: en tiempo real que notifica en caso de un alto consumo de recursos antes de que se presente una falla.*
- *Monitoreo externo: desde servidores externos con notificación de caídas en tiempo real (al supervisor del contrato si lo solicita) y evidencia en un log de auditoría del uptime de cada servicio.*
- *Uptime: Mínimo de 99.6%*
- *Gestión de DNS a solicitud de la entidad de ser requerido.*
- *Firewall: con filtros de red básicos de entrada y de salida, usando restricción de puertos hacia IPs específicas o por rangos.*

4. *Se debe seguir con los procedimientos de buenas prácticas de programación y la normatividad del código de buenas prácticas y desarrollo de software, igualmente la normatividad ISO 27000 y sus sub-series, con la cual se asegura la confidencialidad, Integridad y disponibilidad de los datos contenidos en el Portal Institucional del Fondo de Bienestar Social de la CGR y su base de datos.*

5. *Dar cumplimiento de la política de tratamiento de información del Fondo de Bienestar Social de la CGR, en su calidad de tercero autorizado para el manejo de la información no está autorizado el intercambio de los datos almacenados en la base de datos del aplicativo, en caso de requerirse intercambio de información con algún ente de control o proceso jurídico, este intercambio debe ser autorizado por la Representante legal del Fondo de Bienestar Social de la CGR.*

6. *La empresa debe contar con dos Ingenieros de sistemas, uno de ellos con especialización en gerencia de proyectos y experiencia como ingeniero de proyecto web de un año. Otro ingeniero con experiencia de un año en implementación de portales web bajo esquema manual de Gobierno Digital.*

2.7 Acuerdos de niveles de servicios (ANS)

- MICROSITIOS S.A.S. tendrá un tiempo máximo de 8 horas hábiles para generar reportes y extraer datos para la presentación de informes a entidades externas y entidades de control este tiempo inicia a partir del momento de realizar el registro formal de la solicitud, en la solicitud se deberá anexar plantilla para generar datos.
- MICROSITIOS S.A.S. tendrá un tiempo máximo de 6 horas hábiles para clasificar y dar respuesta a cualquier solicitud de ajustes a la aplicación y/o a su base de datos presentada por el FONDO DE BIENESTAR SOCIAL DE LA CGR.
  Las solicitudes se clasificarán en sencillas, medianas o complejas de acuerdo con el grado de complejidad requerido para su solución completa. Una solución sencilla tendría un plazo máximo de 16 horas hábiles, contadas desde el reporte de la solicitud. Una solución mediana, tendrá un plazo de 24 horas y una solución compleja tendrá hasta 36 horas hábiles.
- MICROSITIOS S.A.S. tendrá un tiempo máximo de 8 horas hábiles luego de clasificar la solicitud para solucionar errores que presente la aplicación, contadas a partir de la hora de remisión del error.
  Se define también un periodo de pruebas de hasta 48 horas hábiles con el fin de validar los ajustes en el portal institucional del Fondo de Bienestar Social de la CGR, este periodo de tiempo se debe discutir con los líderes de las áreas involucradas en los procesos.

Horario de atención de 8:00 a 17:00 horas los días hábiles.

2.8 Obligaciones del contratista:

- *Cumplir a cabalidad con el objeto contractual.*
- *Ejecutar el contrato cumpliendo con todas y cada una de las especificaciones técnicas exigidas.*
- *Durante toda la ejecución del contrato debe mensualmente acreditar que se encuentra al día en el pago de aportes al sistema de seguridad social en salud, pensión y ARL como trabajador independiente, para lo cual debe enviar la planilla de pago correspondiente.*
- *Cada mes debe presentar al supervisor del contrato informe de actividades desarrolladas, en el cual se especifique el avance de esta.*
- *Diligenciar los formatos SICME establecidos para el desarrollo de las actividades.*
- *Mantener informado al supervisor de las novedades de avance de información, dificultades para la recopilación y análisis de esta, variaciones de las condiciones de seguridad establecidas o de la plataforma que conforma el soporte tecnológico de la entidad.*
- *Aceptar la Cláusula de confidencialidad La información contenida en los discos duros de los servidores y bases de datos es de uso exclusivo del Fondo de Bienestar Social de la Contraloría General de la República, por este motivo el CONTRATISTA deberá aceptar la cláusula de confidencialidad y acuerdos de manejo de la información de conformidad con la ley 1273 del 5 de enero de 2009, ley estatutaria 1581 DE 2012, Cumplimiento del artículo 10 del Decreto 1377 de 2013, por medio del cual se reglamenta la Ley Estatutaria 1581 de 2012, y las que se encuentren vigentes a la fecha de firma del contrato.*
- *Mantener la reserva sobre la información que le sea suministrada para el desarrollo del objeto del contrato.*
- *Realizar la facturación electrónica de los correspondientes honorarios conforme le sea indicado por la Entidad, en caso de que, por disposición normativa en materia tributaria, llegare a requerirse.*
- *Suscribir el acta de cumplimiento de la política de tratamiento de información del Fondo de Bienestar Social de la CGR.*
- *Todas las demás obligaciones relacionadas con el objeto del contrato y que no le sean contrarias a éste.*

(…)

8.1 Garantía Técnica

- *La garantía técnica debe cubrir todos los procedimientos ofrecidos, por defecto de las rutinas desarrolladas o ajustadas dentro del Portal Institucional del Fondo de Bienestar Social de la CGR.*

- *El término de la garantía técnica no podrá ser inferior a: cuatro (4) meses contados a partir del recibo a satisfacción, el que constará en el acta respectiva suscrita por el supervisor del contrato.*

- *En consecuencia, el contratista se obliga a realizar las modificaciones al Portal Institucional del Fondo de Bienestar Social de la CGR requeridas para su correcto y óptimo funcionamiento, prestar el soporte técnico y capacitación requerida por parte de los usuarios en los desarrollos o ajustes realizados al Portal Institucional del Fondo de Bienestar Social de la CGR."*

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1. ORDENAR la contratación directa para "Adelantar el mantenimiento del software portal institucional", con la empresa MICROSITIOS S.A.S., NIT. 830.083.023-6, por un valor de **OCHENTA Y CINCO MILLONES NOVECIENTOS CUARENTA Y UN MIL PESOS MTCE ($ 85.941.000),** con un plazo de ejecución que ha de contarse a partir de la fecha de firma del acta de inicio sin extenderse del 16 de diciembre de 2022, fecha en la cual se debe haber cumplido con todas las actividades del presente proceso.

ARTÍCULO 2. *Publicidad.* ORDENAR la publicación de la presente Resolución en el Sistema Electrónico de Contratación Pública – SECOP II.

ARTÍCULO 3. *No Procedencia de Recursos.* La presente Resolución rige a partir de su expedición, se entiende notificada en estrados y se ordena su publicación en el Sistema Electrónico de Contratación Pública - SECOP II.

ARTÍCULO 4. *Vigencia.* La presente resolución rige a partir de su fecha de expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D. C, a los veinticinco (25) días del mes de enero de 2022

ORIGINAL FIRMADO
ANA MARÍA ESTRADA URIBE
Gerente

	Nombre	**Firma**	**Cargo**
Aprobó:	José Luis Arciniegas Galindo		Director Administrativo y Financiero
Revisó:	Lidia Ana Hernández Ayala		Asesora de Gerencia
Revisó:	Gladys Gordillo Ramírez		Asesora Jurídica
Revisó:	Luz Mery Portela David		Asesora Financiera.
Revisó:	Alex William Jojoa Fernández		Prof. Espec Sistemas
Revisó:	Alexandra Tirado Prieto		Prof. Espec Contratación.
Proyectó:	Marialejandra Suárez Pinedo		Abogada Contratista