

	FORMATO			
	CERTIFICADO DE VIABILIDAD DEL OBJETO A CONTRATAR			
	Código: GP-FT-07	Versión: 1	Fecha: 09/03/2023	

1. DATOS DE IDENTIFICACIÓN

1.1 MUNICIPIO(S) O POBLACIÓN BENEFICIADA CON LA EJECUCIÓN DEL PROYECTO:

Directa: Corporación Autónoma Regional del Atlántico – C.R.A.

Indirecta: Población del Departamento del Atlántico.

1.2 OBJETO DEL PROYECTO: PRESTACIÓN DE SERVICIOS PARA LA OPERACIÓN, ADMINISTRACIÓN, MONITOREO, SEGURIDAD, CONTINUIDAD, SOPORTE Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA, DE TELECOMUNICACIONES, DE INFORMACIÓN Y DEL SOFTWARE BASE DEL DATA CENTER DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL ATLÁNTICO – C.R.A.

1.3 PLAZO DE EJECUCIÓN DEL PROYECTO A CONTRATAR: De acuerdo con el plazo establecido en los Estudios Previos.

1.4 VALOR (ESTIMADO) DEL PROYECTO A CONTRATAR: OCHOCIENTOS TREINTA Y NUEVE MILLONES SETECIENTOS CATORCE MIL CIENTO VEINTINUEVE PESOS (\$839.714.129,00), desagregado como se relaciona a continuación:

TIPO GASTO	IDENTIFICACIÓN PRESUPUESTAL	VALOR SOLICITADO
Inversión - GOI	Gastos operativos de inversión para la vigencia 2026.	\$ 399.714.219
Inversión	3.36.07.01.01	\$ 440.000.000
TOTAL		\$ 839.714.129

Los valores se encuentran amparados con el CDP No. 1 del 2 de enero del 2026, el cual se expidió por mayor valor; es decir, por valor de SIETE MIL NOVECIENTOS DIECINUEVE MILLONES NOVECIENTOS NOVENTA Y NUEVE MIL DOSCIENTOS VEINTISEIS PESOS M/CTE (\$ 7.919.999.226) y el CDP No. 282 del 22 de mayo del 2026, Se valida con la Subdirección Financiera que el CDP aún cuenta con recursos por comprometer que amparan el valor solicitado.

2. ARTICULACIÓN CON EL PLAN DE ACCIÓN INSTITUCIONAL: (Vigencia del Plan -años 2024 – 2027)

Línea estratégica 6. Fortalecimiento y Modernización de la Institucionalidad Ambiental				
Programa	Proyecto	Acción Estratégica	Descripción de la Meta Programada	Meta a Contratar
6.2. Tecnologías de la información para el fortalecimiento y desarrollo de la transformación digital de la entidad.	6.2.2 Fortalecer la Seguridad de la Información.	6.2.2.1 Fortalecimiento de la Seguridad de la Información y Ciberseguridad.	Cuatro (4) Herramientas de Ciberseguridad implementadas y mantenidas.	Cuatro (4) Herramientas de Ciberseguridad implementadas y mantenidas.
			Ochenta (80%) de cumplimiento a la estrategia de monitoreo de los servicios tecnológicos.	Ochenta (80%) de cumplimiento a la estrategia de monitoreo de los servicios tecnológicos.

3. VERIFICACIÓN DEL CUMPLIMIENTO DE LAS METAS CON LA EJECUCIÓN DE LAS

Página 1 de 6		
Elaboró:	Revisó:	Aprobó:
Rafael Moreno Álvarez	Juan Camilo Calderón Beltrán	Comité Institucional de Gestión y desempeño

	FORMATO			
	CERTIFICADO DE VIABILIDAD DEL OBJETO A CONTRATAR			
	Código: GP-FT-07	Versión: 1	Fecha: 09/03/2023	

OBLIGACIONES DEL PROYECTO A CONTRATAR / CORRESPONDENCIA DE LA ACCIÓN ESTRATÉGICA Y EL RUBRO PRESUPUESTAL ASIGNADO:

Rubro Presupuestal Asignado (Código de Acción Estratégica)	Meta del PAI a contratar o convenir	Identificación de la Obligación que da cumplimiento a la Meta	La Meta se cumple con la ejecución de la Obligación contractual		El Rubro presupuestal corresponde con la Acción Estratégica	
			SI	NO	SI	NO
6.7.1.1.	Cuatro (4) Herramientas de Ciberseguridad implementadas y mantenidas.	Obligaciones establecidas en el anexo de los Estudios Previos para cada uno de los contratistas de apoyo.	X		X	
6.7.1.1.	Ochenta (80%) de cumplimiento a la estrategia de monitoreo de los servicios tecnológicos.	Obligaciones establecidas en el anexo de los Estudios Previos para cada uno de los p contratistas de apoyo.	PARCIAL		X	

Revisada la información antes relacionada, se considera que las obligaciones específicas del proyecto a contratar contribuirán con el cumplimiento de la(s) meta(s) antes señalada(s); y, que existe correspondencia entre la Acción Estratégica y el (los) Rubro(s) presupuestal(es) asignado(s) para llevar a cabo la contratación de este PROYECTO INSTITUCIONAL.

SI (X) NO ()

4. OBSERVACIONES:

La Corporación Autónoma Regional del Atlántico – C.R.A., entidad pública de la orden nacional creada por la Ley 99 de 1993, tiene como objeto principal la administración de los recursos naturales renovables y el medio ambiente en su jurisdicción departamental, con sede principal en la ciudad de Barranquilla.

En el ejercicio de sus funciones, la C.R.A. se enfrenta a un entorno de crecientes amenazas cibernéticas y riesgos operacionales que pueden comprometer la seguridad, la continuidad del servicio y la confidencialidad de la información institucional. La materialización de incidentes (vulnerabilidades explotadas, malware/ransomware, fallas de infraestructura, errores de configuración o indisponibilidad de plataformas críticas) puede generar afectación de la operación, interrupción de servicios institucionales, pérdida o corrupción de información y riesgos reputacionales y legales. En consecuencia, y en el marco de la responsabilidad de la Oficina Asesora de Ciencia, Tecnología e Innovación – CTel de controlar los riesgos asociados a las TIC, la entidad requiere fortalecer y asegurar de manera continua capacidades especializadas de gestión, monitoreo, análisis, recuperación, continuidad y optimización de su infraestructura tecnológica, incorporando componentes de ciberseguridad que permitan asegurar la disponibilidad, rendimiento y protección de la infraestructura y la información frente a incidentes y amenazas digitales.

La C.R.A. cuenta con una infraestructura tecnológica propia en operación que demanda administración especializada y monitoreo permanente, compuesta por una red LAN basada en

Página 2 de 6		
Elaboró: Rafael Moreno Álvarez	Revisó: Juan Camilo Calderón Beltrán	Aprobó: Comité Institucional de Gestión y desempeño

	FORMATO			
	CERTIFICADO DE VIABILIDAD DEL OBJETO A CONTRATAR			
	Código: GP-FT-07	Versión: 1	Fecha: 09/03/2023	

cableado estructurado UTP Categoría 6A con anchos de banda 10/100/1000 Mbps y up-link de 10 Gbps, un switch Core Dell EMC S4128F que interconecta el Datacenter, la red inalámbrica y los switches de borde (2 switches HP V1910 de 48 puertos, 1 switch HP V1910 de 24 puertos, 1 switch 3COM V2928 de 24 puertos, 1 switch DELL N2048P de 48 puertos, 1 switch DELL EMC N1148T-ON y 1 switch DELL EMC N1124T-ON). Así mismo, la CRA dispone de un Datacenter corporativo en producción con servidores tipo RACK (2 servidores Dell R520 con procesador Intel Xeon CPU E5-2440 v2 @ 1.90GHz 8C/16T, 96 GB RAM, disco de 500 GB; y 1 servidor DELL EMC R740 con 256 GB RAM, 18C/36T, 4x Ethernet 10Gbps SFP+, 2x SSD 480), gestionados con VMWARE ESSENTIALS PLUS y VMware vCenter Server 6 Foundation, infraestructura de almacenamiento Dell PowerVault MD3600i de 10 TB y SAN Dell Compellent EMC 3020 de 30 TB, además de dos switches TOR para SAN DELL EMC S4112F en alta disponibilidad. Adicionalmente, la entidad dispone de una plataforma de red inalámbrica FortiAP integrada al firewall, contando con un firewall Fortigate 100F para seguridad WAN-LAN en su sede principal.

La infraestructura de redes y seguridad de la Entidad está soportada en soluciones tecnológicas de los fabricantes Fortinet, incluyendo la plataforma de red inalámbrica (WiFi) y Antivirus Kaspersky Next EDR Optimum. En este contexto, se hace necesario contar con servicios especializados prestados por profesionales certificados en estas tecnologías, que permitan realizar la administración, el monitoreo, el mantenimiento y el soporte técnico de dichas soluciones. Lo anterior garantiza la continuidad operativa, la disponibilidad de los servicios tecnológicos y el fortalecimiento de la postura de ciberseguridad de la Entidad.

Así mismo, en la actualidad la Corporación tiene implementado y licenciado el software de seguridad de Antivirus, Kaspersky Next EDR Optimum, para 300 usuarios y una consola de administración con el propósito de proteger los equipos de cómputo – endpoints de la corporación - C.R.A.

De igual forma, la infraestructura tecnológica del Centro de Datos de la Entidad se encuentra implementada sobre plataformas del fabricante Dell, conformadas por servidores, sistemas de almacenamiento y equipos de conmutación (switches), los cuales constituyen la base para la operación de los sistemas de información, servicios de red y aplicaciones institucionales. En consecuencia, resulta necesario contar con servicios especializados para su administración, monitoreo, mantenimiento preventivo y correctivo, soporte técnico y optimización, garantizando la disponibilidad, continuidad operativa, integridad y desempeño de la infraestructura tecnológica.

En materia de ciberseguridad y operación, la C.R.A. requiere mantener y fortalecer controles técnicos sobre el perímetro, la navegación, el acceso y la protección frente a amenazas, junto con capacidades de respuesta y recuperación ante incidentes. Para ello, resulta necesario disponer de un proveedor integral con capacidades técnicas y operativas para administrar y operar los componentes críticos de seguridad, incluyendo la renovación del licenciamiento del firewall perimetral institucional, su operación y la implementación/configuración de un Web Application Firewall – WAF para proteger aplicaciones web expuestas en Internet, así como la gestión especializada de incidentes, problemas y eventos de Seguridad de la Información, con análisis, documentación, monitoreo, seguimiento y escalamiento.

Que la C.R.A. adquirió recientemente un conjunto de estaciones de monitoreo ambiental, instaladas en diferentes puntos estratégicos del departamento del Atlántico. En desarrollo de sus funciones, la Entidad tiene la responsabilidad de recibir, almacenar, custodiar y garantizar la disponibilidad de la información generada por dichas estaciones, para lo cual se requiere la incorporación del servidor destinado al acopio de esta información dentro de la infraestructura tecnológica del Data Center institucional.

En consecuencia, es necesario realizar la integración del servidor al entorno del Data Center, incluyendo su configuración e integración con la infraestructura existente, la implementación de

Página 3 de 6		
Elaboró: Rafael Moreno Álvarez	Revisó: Juan Camilo Calderón Beltrán	Aprobó: Comité Institucional de Gestión y desempeño

	FORMATO			
	CERTIFICADO DE VIABILIDAD DEL OBJETO A CONTRATAR			
	Código: GP-FT-07	Versión: 1	Fecha: 09/03/2023	

controles de acceso, la aplicación de medidas de seguridad de la información, la habilitación de los servicios tecnológicos requeridos y la configuración de los mecanismos de respaldo y recuperación de la información, con el fin de garantizar la disponibilidad, integridad, confidencialidad y continuidad de la información recolectada por las estaciones de monitoreo.

De igual forma en su proceso de optimización de la infraestructura la entidad adquirió recientemente, mediante un proceso de contratación independiente, un canal de Internet dedicado de respaldo de 500 Mbps sobre fibra óptica, con el propósito de fortalecer la disponibilidad y continuidad de los servicios de conectividad institucional.

Para que este servicio pueda ser utilizado de manera eficiente y cumpla con el propósito para el cual fue adquirido, es necesario realizar su integración a la infraestructura tecnológica de la Entidad, específicamente al centro de cableado y a la plataforma de seguridad perimetral (Firewall), mediante la configuración e implementación de mecanismos de balanceo de carga y/o alta disponibilidad (failover), según la arquitectura tecnológica existente.

Estas actividades comprenden la configuración de interfaces, rutas, políticas de seguridad, reglas de enrutamiento, traducción de direcciones (NAT), monitoreo del estado de los enlaces y demás parámetros técnicos necesarios para garantizar la interoperabilidad entre ambos canales de Internet, permitiendo la conmutación automática ante fallas del enlace principal o la distribución del tráfico cuando la arquitectura lo permita.

La implementación de esta solución permitirá incrementar la disponibilidad de los servicios tecnológicos institucionales, reducir el riesgo de indisponibilidad por fallas en la conectividad, garantizar la continuidad de los servicios críticos soportados sobre la infraestructura tecnológica y mejorar la resiliencia de la red institucional frente a incidentes o interrupciones del servicio de Internet.

Que la Entidad dispone de 2 sedes administrativas ubicadas en diferentes puntos geográficos, las cuales requieren la implementación de una solución de interconexión telemática que permita integrar sus redes locales de manera segura, garantizando la transmisión de datos y voz sobre una infraestructura con segmentación mediante VLAN, priorización y optimización del tráfico en doble vía (QoS), fortaleciendo la seguridad de las comunicaciones, la disponibilidad de los servicios, la continuidad operativa y el acceso eficiente a los recursos tecnológicos compartidos, por lo tanto se requiere de la implementación de una LAN extendida, necesaria para el cumplimiento de las funciones misionales y administrativas de la Corporación.

Que la Corporación Autónoma Regional del Atlántico – C.R.A., en desarrollo de su proceso de modernización de la infraestructura tecnológica y con el propósito de fortalecer sus servicios institucionales de comunicaciones, requiere implementar una plataforma de telefonía IP basada en tecnología Asterisk, la cual será instalada sobre un servidor del Data Center institucional, permitiendo centralizar y administrar las comunicaciones de voz de la Entidad.

Como parte de esta implementación, la Entidad requiere la configuración e integración de una nueva troncal SIP suministrada por el operador de telecomunicaciones, la cual permitirá establecer la comunicación entre aproximadamente ciento veinte (120) extensiones de voz sobre IP distribuidas entre las sedes 1 y 2, garantizando un servicio de telefonía moderno, escalable y administrable.

La implementación de esta solución demanda servicios especializados para la instalación, configuración, parametrización, integración y puesta en operación de la plataforma de telefonía IP y de la troncal SIP, incluyendo la definición del plan de numeración, configuración de extensiones, reglas de enrutamiento de llamadas, perfiles de usuarios, autenticación, interoperabilidad con el proveedor del servicio, configuración de codecs, parámetros de calidad del servicio (QoS), políticas de seguridad, así como la realización de pruebas funcionales, de conectividad y de estabilidad que garanticen el correcto funcionamiento de la solución.

Página 4 de 6		
Elaboró: Rafael Moreno Álvarez	Revisó: Juan Camilo Calderón Beltrán	Aprobó: Comité Institucional de Gestión y desempeño

	FORMATO			
	CERTIFICADO DE VIABILIDAD DEL OBJETO A CONTRATAR			
	Código: GP-FT-07	Versión: 1	Fecha: 09/03/2023	

La contratación de estos servicios especializados permitirá disponer de una plataforma institucional de comunicaciones unificadas integrada a la infraestructura tecnológica del Data Center, optimizando las comunicaciones entre las diferentes sedes de la Entidad, reduciendo la dependencia de soluciones tradicionales de telefonía, mejorando la administración del servicio y garantizando la disponibilidad, continuidad, escalabilidad y eficiencia de las comunicaciones de voz institucionales.

Que la entidad se encuentra adelantando acciones orientadas al fortalecimiento de su Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de adoptar las mejores prácticas internacionales en materia de seguridad de la información y avanzar en el cumplimiento de los requisitos establecidos en la familia de normas ISO/IEC 27000, especialmente la ISO/IEC 27001. En este contexto, resulta necesario implementar y fortalecer los controles técnicos, administrativos y operativos sobre la infraestructura tecnológica, las plataformas de información y los servicios digitales, como parte del proceso de preparación institucional para una futura certificación, así como para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

En consecuencia, la contratación de servicios especializados para la administración, configuración, monitoreo y fortalecimiento de la infraestructura tecnológica y de ciberseguridad constituye un componente esencial para la implementación y madurez de los controles del Sistema de Gestión de Seguridad de la Información (SGSI), contribuyendo al cierre de brechas identificadas y al avance del proceso institucional hacia el cumplimiento de los requisitos de la norma ISO/IEC 27001.

De igual forma, la C.R.A. requiere asegurar la continuidad del negocio mediante un servicio integral de copias de seguridad y recuperación que cubra endpoints, servidores y servicios de Microsoft 365, bajo un esquema que incluya gestor de Backup como servicio (SaaS) y almacenamiento en la nube aprovisionado por el proveedor, garantizando integridad de datos y capacidad de restauración ante fallas o incidentes de seguridad. Complementariamente, se requiere soporte especializado para la actualización, aseguramiento y mantenimiento de dominios (locales e Internet), Directorio Activo y servicios en Azure Cloud como base de la infraestructura de identidades y servicios institucionales, así como servicios de mantenimiento, soporte, asistencia técnica e instalación del software base del Datacenter, y mantenimiento preventivo/correctivo de dispositivos y sistemas del Datacenter (servidores, almacenamiento, UPS, aires de precisión, tableros eléctricos y demás infraestructura asociada).

Para asegurar la correcta operación y continuidad de los servicios tecnológicos institucionales, la entidad requiere que el contratista preste asistencia técnica y especializada integrada con la mesa de ayuda institucional (Kaía), enfocada en soportes de nivel III y IV sobre la infraestructura de procesamiento, almacenamiento y networking, y sobre la gestión de incidentes de Seguridad de la Información, con el fin de garantizar la continuidad, disponibilidad y seguridad de los servicios tecnológicos institucionales conforme a buenas prácticas de gestión de servicios.

En consecuencia, la C.R.A. requiere contratar un proveedor integral que preste un servicio gestionado, con niveles de servicio, orientado a la operación y administración de la infraestructura tecnológica y de los controles de ciberseguridad descritos, cuyo alcance específico se definirá en el anexo técnico correspondiente.

Para la contratación se cuenta con certificación donde consta que el personal de planta de la Corporación es insuficiente para atender las actividades señaladas anteriormente.

La presente contratación se encuentra incluida en el Plan Anual de Adquisiciones con el siguiente objeto “PRESTACIÓN DE SERVICIOS PARA LA OPERACIÓN, ADMINISTRACIÓN, MONITOREO, SEGURIDAD, CONTINUIDAD, SOPORTE Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA, DE TELECOMUNICACIONES, DE INFORMACIÓN Y DEL SOFTWARE BASE DEL

Página 5 de 6		
Elaboró: Rafael Moreno Álvarez	Revisó: Juan Camilo Calderón Beltrán	Aprobó: Comité Institucional de Gestión y desempeño

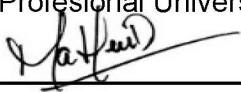
	FORMATO			
	CERTIFICADO DE VIABILIDAD DEL OBJETO A CONTRATAR			
	Código: GP-FT-07	Versión: 1	Fecha: 09/03/2023	

DATA CENTER DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL ATLÁNTICO – C.R.A.” en la clasificación UNSPSC 80161500.

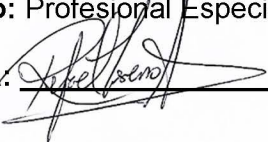
Verificada la información de los Estudios previos y rubro de los CDP No. 01 del 02 de enero del 2026 y No. 282 del 22 de mayo de 2026, se valida que existe correspondencia entre las obligaciones y las metas a cumplir con la ejecución del proyecto a contratar, toda vez que, con las acciones a desarrollar a través del objeto se contribuye a dar cumplimiento a las metas programadas.

Como constancia de lo anterior, se firma este documento a los 19 días del mes de agosto del año 2026.

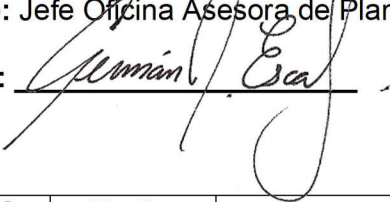
ELABORADO POR: Madeleine Hernández Duva
Cargo: Profesional Universitario

Firma: 

NOMBRE DE QUIEN VALIDA LA INFORMACIÓN: Rafael Moreno Álvarez
Cargo: Profesional Especializado

Firma: 

NOMBRE DE QUIEN APRUEBA: Germán Escaf Payares
Cargo: Jefe Oficina Asesora de Planeación

Firma: 

Versión	Fecha	Descripción del Cambio
1	09/03/2023	Creación del documento