RESOLUCIÓN NÚMERO (1049-2026) MD-DIMAR-SUBAFIN-GINREDCE 18 DE SEPTIEMBRE DE 2026

POR MEDIO DE LA CUAL SE ORDENA LA APERTURA DEL PROCESO DESELECCIÓN ABREVIADA DE MENOR CUANTIA No. 346-GINREDCE-2026

El Coordinador del Grupo Intendencia Regional Central de la Dirección General Marítima, debidamente nombrado para celebrar contratos, mediante Resolución No. 0846-2026 MD-DIMAR-SUBAFIN-GRUDHU 11 DE AGOSTO DE 2026, facultado para ejercer las funciones y competencias relacionadas con la contratación de prestación de bienes y servicios destinados a la Dirección General Marítimaen virtud de la Resolución de Delegación No. 4223 del 23 de junio de 2022 por medio de lacual se delegan unas funciones y competencias relacionadas con la Contratación de Bienesy Servicios con destino al Ministerio de Defensa Nacional, y de conformidad con lo establecido en la Resolución No. 4130 de 16 de junio de 2022 Manual de Contratación y Convenios del Ministerio de Defensa Nacional y, en especial las que le confiere la Ley 80 de1993, la Ley 1150 de 2007 y sus Decretos reglamentarios, ha determinado dar inicio al presente proceso de contratación, el cual se regirá bajo los siguientes parámetros y

CONSIDERANDO:

Que el Ministerio de Defensa Nacional - Dirección General Marítima – Grupo Intendencia Regional Central, de conformidad con la ejecución de sus funciones, requiere contratar la **"ADQUISICIÓN DEL LICENCIAMIENTO DE LAS HERRAMIENTAS DE SEGURIDAD, MONITOREO Y SERVICIOS PARA LA DIMAR, CONFORME CON LAS ESPECIFICACIONES ESTABLECIDAS EN EL ANEXO TÉCNICO",** hasta por la suma de **MIL DOSCIENTOS CUARENTA Y SEIS MILLONES TRESCIENTOS SESENTA Y SEIS MIL QUINIENTOS CUARENTA Y CINCO PESOS ($1.246.366.545,00)** incluido IVA (cuando aplique) y las demás erogaciones que correspondan**,** de acuerdo con el Certificado de Disponibilidad Presupuestal CDP No. **47126 del 30 de julio del 2026** expedido por la Sección de Presupuesto de la GINREDCE, así:

No. CDP	Tipo Gasto	Rec	C/S	CONCEPTO	AFECTADO EN
47126	A-02-01-01-004-007	16	SSF	A-02-02-01-004-007 EQUIPO Y APARATOS DE RADIO, TELEVISIÓN Y COMUNICACIONES	948.812.878
47126	C-1599-0100-1-20109G-1599076-02	16	SSF	C-1599-0100-1-20109G-1599076-02 ADQUIS. DE BYS - SERVICIOS TECNOLÓGICOS - CONSOLIDACIÓN DEL POTENCIAL DE LAAUTORIDAD MARÍTIMA EN EL TERRITORIO NACIONAL	297.553.667
				TOTAL PRESUPUESTO	1.246.366.545

Detallado por lotes de la siguiente manera:

Ítem	Lotes	Descripción técnica del bien y/o servicio requeridos	Valor	Rubro
1.1	Lote 1	Imperva **Incapsula Enterprise** 20Mbps 30 Website included.Anual Incapsula Subscription; Includes 5 Login Protect user licenses	$344.980.700,00	A.02.02.01.004.007

Ítem	Lotes	Descripción técnica del bien y/o servicio requeridos	Valor	Rubro
		Includes 1Gbps of DDoS protection. TERM 1 YEAR Soporte local 7x24		
2.1	Lote 2	Licencia Monitoreo **TENABLE IO**.	$47.921.950,00	A.02.02.01.004.007
3.1	Lote 3	Adquisición del software **Kaspersky** Next Edr Optimum	$72.125.625,00	A.02.02.01.004.007
4.1	Lote 4	Suscripción Licenciamiento solución **DLP** (RTERAMIND) x 1 año.	$ 135.089.925,00	C-1599-0100-1-20109G-1599076-02
4.2		Suscripción Licenciamiento solución **PAM** (Segura) x 1 año.	$25.466.150,00	C-1599-0100-1-20109G-1599076-02
5.1	Lote 5	Licenciamiento Herramienta de encriptación.	$60.215.404,00	C-1599-0100-1-20109G-1599076-02
5.2		Servicio de implementación herramienta de encriptación.	$46.817.988,00	C-1599-0100-1-20109G-1599076-02
6.1	Lote 6	Servicios de **Hardening** para Office 365	$29.964.200,00	C-1599-0100-1-20109G-1599076-02
7.1	Lote 7	Adquisición de Licenciamiento - Plataforma de Cibervigilancia y Ciberinteligencia (**Kartos**) x 1 año	$483.784.603,00	A.02.02.02.008.003
		Valor total del presupuesto oficial	$ 1.246.366.545,00	

Los Ítems 1.1, 2.1, 3.1, 4.1, 4.2, 5.1 y 7.1 ***se encuentran*** *exentos de IVA de conformidad con lo establecido en el literal N del numeral 3 del artículo 477 del Estatuto Tributario.*

Tratamiento de IVA - Estatuto tributario:
Artículo 477. Bienes que se encuentran exentos del impuesto. Están exentos del impuesto sobre las ventas, con derecho a compensación y devolución, los siguientes bienes:
(…)
3. Las municiones y material de guerra o reservado y por consiguiente de uso privativo y los siguientes elementos pertenecientes a las Fuerzas Militares y la Policía Nacional:
(…)
n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional

El ítem 1.1 corresponde a una solución Web Aplication Firewall, cuya naturaleza técnica es la de una plataforma de seguridad web operada en la nube bajo modalidad de suscripción. Su funcionalidad radica en la inspección lógica del tráfico, protección contra ataques y gestión de aplicaciones mediante reglas programadas y analítica digital. No existe entrega de infraestructura física, sino acceso a un entorno tecnológico mediante licenciamiento. En consecuencia, se trata de software orientado a sistemas y comunicaciones, subsumible en la exención del IVA prevista en el artículo 477 del Estatuto Tributario.

El ítem 2.1 corresponde a Tenable IO VM, una plataforma destinada a la identificación, análisis y gestión de vulnerabilidades sobre activos tecnológicos. Su operación se basa en motores de escaneo, procesamiento de datos, generación de reportes y visualización mediante consola y servicios API, todo bajo esquema de licenciamiento. Desde el punto de vista técnico, es inequívocamente software, en tanto no implica bienes físicos sino procesamiento lógico de información, por lo cual encuadra en el concepto de software de sistemas cubierto por la exención tributaria.

El ítem 3.1 hace referencia a la solución Kaspersky EDR, la cual constituye un software de seguridad para endpoints con capacidades avanzadas de detección y respuesta ante incidentes. Su estructura comprende agentes instalables, consola de administración y servicios en la nube, todos licenciados para su uso. Se trata de un producto puramente lógico que opera sobre sistemas informáticos, razón por la cual se clasifica como software de seguridad informática y se encuentra dentro del alcance de la exención del IVA.

El ítem 4.1 corresponde a una solución DLP (Data Loss Prevention), cuya finalidad es prevenir la fuga de información mediante el monitoreo, análisis y control del comportamiento digital de los usuarios. Sus capacidades incluyen grabación de actividad, análisis OCR, políticas de seguridad y generación de alertas, todo basado en procesamiento de datos y reglas lógicas. Esta naturaleza evidencia que se trata de software especializado en protección de información, por lo cual es susceptible de la exención establecida en la norma.

El ítem 4.2 se refiere a una solución PAM (Privileged Access Management), orientada a la gestión de accesos privilegiados, credenciales y sesiones dentro de la infraestructura tecnológica. Funciona mediante módulos de autenticación, control de acceso, auditoría y administración centralizada, todos implementados a través de software. Al tratarse de un sistema lógico que administra la seguridad de los accesos en entornos informáticos, se clasifica como software de sistemas y comunicaciones y, en consecuencia, se encuentra amparado por la exención del IVA.

El ítem 5.1 corresponde a una herramienta de encriptación, la cual implementa algoritmos criptográficos para proteger la información mediante cifrado, control de acceso y gestión de políticas sobre datos digitales. Su operación es completamente lógica, sin componentes físicos asociados, y orientada a la seguridad de la información institucional. Por tanto, se trata de software en sentido estricto, incluido dentro de los bienes exentos conforme al artículo 477 del Estatuto Tributario.

Finalmente, el ítem 7.1 consiste en una plataforma de ciberinteligencia (Kartos) en modalidad SaaS, que integra múltiples capacidades de monitoreo, análisis y gestión de riesgos digitales a través de una arquitectura en nube. Su funcionamiento es completamente automatizado y basado en procesamiento de información mediante algoritmos y módulos de software. En consecuencia, corresponde claramente a software de sistemas y comunicaciones, lo que permite su inclusión dentro del supuesto de exención del IVA contemplado en el artículo 477 del Estatuto Tributario.

Que conforme a los numerales 4 y 12 del artículo 25 de la Ley 80 de 1993, modificado por elartículo 87 de la Ley 1474 del 12 de Julio de 2011, artículo 8 de la Ley 1150 de 2007, y decreto 1082 de 2015, el Señor **CF FRANCISCO JOSE VILLEGAS PÉREZ Coordinador del Grupo TIC** de la Dirección General Marítima – DIMAR, elaboró el estudio previo de fecha 28 de agosto del 2026, confirmando la existencia de la partida presupuestal requerida respaldado en el Certificado de Disponibilidad Presupuestal No. 47126 del 30 de julio del 2026, con el fin de contratar la, con fundamento en las siguientes argumentaciones:

"El Grupo TIC (GRUTIC) de DIMAR tiene como responsabilidad principal dirigir la estrategia y el desarrollo del portafolio de proyectos y servicios de Tecnologías de la Información y Comunicaciones (TIC), alineados con la normativa vigente, las necesidades institucionales y la arquitectura empresarial. Esto incluye la definición de políticas y lineamientos de TIC, así como la gestión de proyectos y la operación de los servicios de TIC.

Dentro de los objetivos planteados, se incluye:

a) *El monitoreo y control de las visitas a las publicaciones web de la Entidad, las cuales constituyen un blanco frecuente para diversos tipos de ataques cibernéticos. En este sentido, se propone un complemento adecuado a la infraestructura tecnológica de la Dirección General Marítima (DIMAR), mediante la implementación de sistemas informáticos avanzados, servicios especializados y elementos técnicos que permitan abordar eficientemente los desafíos relacionados con los ataques a la seguridad informática. Esto se logrará a través de controles estrictos de confidencialidad, integridad y disponibilidad de las plataformas tecnológicas, todo ello fundamentado en el monitoreo constante, el seguimiento proactivo y la mitigación de los impactos derivados de los ataques informáticos.*

El enfoque integral se basa en la utilización de tecnología de software de protección avanzada, junto con metodologías que incluyen un seguimiento físico de los sitios web, de acuerdo con los lineamientos establecidos por las normativas sectoriales, con el objetivo de garantizar la seguridad de los servicios informáticos, las plataformas tecnológicas y la información crítica de DIMAR, que opera como una unidad adscrita al Ministerio de Defensa Nacional.

En este contexto, la necesidad de realizar esta adquisición se justifica por la necesidad de asegurar el desempeño óptimo y la escalabilidad de la plataforma tecnológica de la Entidad, para no solo soportar los servicios actuales, sino también para facilitar su crecimiento a medida que se implementen los planes estratégicos del área de Tecnologías de la Información. Esta solución garantizará que los recursos y las publicaciones generadas por este proyecto sean respaldados adecuadamente, asegurando el cumplimiento de los compromisos institucionales en su rol como autoridad marítima de Colombia.

El propósito fundamental de estas herramientas es fortalecer las estrategias de ciberseguridad y ciberdefensa, orientadas a prevenir, controlar y mitigar los efectos de los ataques informáticos, en particular los ataques de Denegación de Servicios (DDoS) y otras amenazas a los sitios web. Para ello, se implementará un esquema de seguridad informática basado en software licenciado para el monitoreo constante y el soporte técnico, lo que permitirá reducir significativamente los riesgos asociados a la seguridad cibernética y contar con una respuesta eficiente ante los incidentes, gracias a la colaboración con empresas especializadas en el ámbito de la seguridad informática.

Teniendo en cuenta que durante años se ha trabajado con licenciamiento Imperva, los ingenieros de seguridad ya cuentan con experiencia en la herramienta y que esta a su vez ya se encuentra parametrizada bajo las necesidades de la Entidad, por tanto se hace necesario dar continuidad al software de esta casa sin incurrir en costos de capacitación e implementación, además del impacto que generaría el cambio a otra solución WAF.

En el caso que no se adelante la adquisición del licenciamiento WAF, las publicaciones de la DIMAR quedaran totalmente expuestas a ataques cibernéticos, posiblemente modificaciones o caídas por ataques de Denegación de Servicios (DDoS), lo cual afectaría la reputación, la información y expondría no sólo a la DIMAR, sino también a sus usuarios a diferentes vulnerabilidades, que podría ser explotadas por un ciber atacante.

b) La ejecución de acciones proactivas y preventivas en el Área Tecnológica. Como una de las más reconocidas, Tenable ha demostrado tener las capacidades necesarias para apoyar al área de seguridad informática en la búsqueda y detección de vulnerabilidades, tanto de servidores, como de estaciones y dispositivos IoT.

Con fundamento en lo expuesto, es importante mencionar que, en caso de no Contratarse la licencia, la perdida de datos, la disponibilidad de los Sistemas de Información y/o pérdida de su monitoreo, así como la Integridad y Confidencialidad de la Información junto con sus activos, pueden verse vulnerados e inseguros debido a la ausencia de soporte, administración y la no aplicación de buenas prácticas que requieren dichos sistemas para funcionar con normalidad.

Además, es crucial resaltar que, de no adquirirse el licenciamiento con la marca TENABLE IO (VM), se tendría que realizar una etapa de implementación y despliegue, lo que implicaría costos adicionales, además de la capacitación del personal y la adaptación en la infraestructura. La falta de una solución de seguridad robusta podría exponer a la organización a riesgos significativos, incluyendo ataques cibernéticos, accesos no autorizados y posibles sanciones regulatorias por incumplimiento de normativas de protección de datos.

c) La la adquisición de software antimalware por un año, ya que esto permite fortalecer la seguridad en la navegación de los usuarios y mitigar el riesgo de múltiples amenazas virtuales que podrían comprometer los sistemas de información de la red.

Por lo tanto, es indispensable renovar las licencias del antimalware en uso, dado que cumplen con los requisitos técnicos y operativos óptimos para la plataforma tecnológica de la DIMAR. Esta renovación no solo protege el hardware y software ante riesgos y amenazas de malware, sino que también contribuye al cumplimiento de la política de seguridad en la protección de datos, previniendo la fuga de información.

En caso de no adquirir la solución con la que se viene trabajando, se genera un periodo de estabilización y aprendizaje de la infraestructura y de los administradores, lo cual además de generar costos adicionales a la Entidad en instalación y despliegue, también representa un riesgo al tener que aprender nuevamente el comportamiento de la red y de los equipos.
Para garantizar la efectividad del software de protección, es fundamental llevar un registro detallado de los eventos e incidentes informáticos dentro de un proceso adecuado de administración y respuesta. Esto requiere el uso de herramientas especializadas en la detección de malware, que permitan analizar la situación y establecer medidas de defensa ante las amenazas. En este contexto, es crucial contar con una solución de software capaz de identificar las causas de los incidentes y diseñar estrategias de protección frente a actores malintencionados, como los ciberterroristas, quienes emplean código malicioso para llevar a cabo ataques contra las entidades.

Con el fin de dar cumplimiento a lo anterior, el Grupo TIC - GRUTIC de la Dirección General Marítima – DIMAR, requiere la renovación de licencias de software antivirus KASPERSKY ENDPOINT DETECTION AND RESPONDE OPTIMUM, para 1350 licencias incluyendo última versión liberada. Esto dará continuidad al licenciamiento e implementación actual, sin requerir implementaciones adicionales, capacitación, estabilización, aprendizaje de la plataforma y otra serie de actividades que no solo implicarían costosa adicionales, sino también tiempo y mientras todas estas se completan, podrían poner en riesgo a la Entidad, cosa que ocurriría de contratarse un Software diferente.

Las licencias de software generalmente no se adquieren por tiempo inferior a 12 meses, por ser un tema especializado sobre la protección de los datos ante ataques informáticos por el uso de software malicioso, el art.269 literal E de la Ley 1273 de 2009, sobre los atentados a la información y los sistemas informáticos, literalmente expresa:

"Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (…)".

Como se puede evidenciar, a partir de la citada norma se genera responsabilidad a la administración de tecnologías de las entidades, respecto a la implementación de controles preventivos y correctivos ante posibles atentados contra la seguridad y uso de software malicioso, por lo que es necesario que la continuidad del funcionamiento y uso de herramientas de software, motivo por el cual es pertinente renovar las licencias de software por 12 meses, a fin de garantizar la continuidad de las herramientas de protección que permitan garantizar a su vez, la seguridad de la información de la Dirección General Marítima.

Es fundamental destacar que, al tratarse de un software crítico para la seguridad de estaciones finales y servidores, la ausencia de esta herramienta puede tener un impacto significativo en la protección de la información, poniendo en riesgo los datos, la infraestructura y los servicios que la Entidad ofrece un control puntual, sino un trabajo continuo, cuyo valor radica precisamente en la supervisión permanente, el análisis especializado y la generación de alertas oportunas. En este sentido, dar continuidad al licenciamiento garantiza la sostenibilidad de los controles implementados, la protección de la reputación institucional y el cumplimiento de los lineamientos estratégicos y normativos en materia de ciberseguridad.

d) Por otro lado, en relación con las soluciones de Gestión de Accesos Privilegiados (PAM) y Prevención de Pérdida de Datos (DLP), la experiencia obtenida durante la operación inicial permitió identificar que el licenciamiento contratado (30 licencias) resulta insuficiente para cubrir de manera integral a todo el personal crítico que hace parte de los equipos de administración de redes, plataformas, bases de datos, infraestructura, seguridad de la información y en general personal que administra datos sensibles, quienes, por la naturaleza de sus funciones, cuentan con accesos privilegiados y manipulan información sensible y estratégica.

La ampliación del licenciamiento PAM es necesaria para garantizar que la totalidad de los accesos privilegiados sean gestionados bajo controles robustos, centralizados y auditables, evitando esquemas mixtos o excepciones operativas que incrementen el riesgo de uso indebido de credenciales, escalamiento de privilegios o movimientos laterales dentro de la infraestructura tecnológica. La solución PAM, basada en buenas prácticas internacionales permite asegurar credenciales críticas, registrar y monitorear sesiones privilegiadas, automatizar la rotación de contraseñas y generar evidencia trazable para auditorías internas y externas. Limitar su cobertura

únicamente a una parte del personal crítico debilita el modelo de control y expone a la Dimar a riesgos operativos y de seguridad innecesarios.

De igual forma, la ampliación del licenciamiento de la solución DLP resulta fundamental para extender la protección de la información sensible a todos los usuarios y equipos que, por su rol, acceden, procesan o administran datos clasificados, estratégicos o sujetos a reserva legal. La cobertura parcial del DLP genera brechas en la capacidad de detección y prevención de fugas de información, especialmente frente a vectores como dispositivos extraíbles, correo electrónico, navegación web y almacenamiento en la nube. Una ampliación del licenciamiento permitirá aplicar políticas homogéneas, consistentes y alineadas con el nivel de riesgo real de la Dimar, fortaleciendo la confidencialidad, integridad y disponibilidad de la información.

Desde el punto de vista normativo y de cumplimiento, la continuidad y ampliación de estas soluciones se encuentra alineada con los requisitos de la ISO 27001:2022, en particular en los dominios relacionados con control de accesos, criptografía, protección de la información, gestión de incidentes y seguridad en la operación, así como con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Ley 1581 de 2012 y el Decreto 1078 de 2015. Asimismo, estas acciones fortalecen la capacidad institucional para responder a auditorías, requerimientos de entes de control y eventuales procesos judiciales, al contar con evidencias técnicas confiables y mecanismos de control formalmente establecidos.

Adicional, En el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y considerando la transición a la versión ISO/IEC 27001:2022, se ha identificado una brecha relevante en la implementación de controles asociados a la protección criptográfica de la información, particularmente en lo relacionado con la confidencialidad y el control de uso de la información sensible fuera del perímetro institucional.

La norma ISO/IEC 27001:2022, en su dominio de controles tecnológicos, establece la necesidad de implementar mecanismos criptográficos adecuados para proteger la información durante todo su ciclo de vida, incluyendo el almacenamiento, la transmisión y el uso, así como de definir políticas claras para la gestión de claves y el control de accesos.

Actualmente, la Dimar carece de mecanismos que permitan ejercer control efectivo sobre la información una vez esta es compartida con usuarios internos o externos, lo que incrementa el riesgo de fuga de información, uso no autorizado, pérdida de confidencialidad y afectación reputacional.

e) La implementación de una solución de protección persistente de la información basada en criptografía, como SealPath, permite dar cumplimiento directo a los controles establecidos en ISO/IEC 27001:2022, al garantizar que:

- *La información se encuentre cifrada de forma permanente, independientemente de su ubicación.*
- *El acceso a los documentos esté estrictamente controlado y autenticado.*
- *Exista capacidad de revocación inmediata del acceso ante incidentes, desvinculación de personal o cambios en el nivel de riesgo.*
- *Se mantenga trazabilidad completa sobre el uso de la información, facilitando auditorías, investigaciones y cumplimiento normativo.*

f) Adicionalmente con el fin de fortalecer las capacidades de la Entidad, en seguridad, usando el licenciamiento de O365 con que cuenta la Entidad, se requiere contar con personal especializado, que realice asesoría e implemente las mejores prácticas y configuraciones, optimizando los recursos actuales, añadiendo capacidades mediante una parametrización adecuada del entorno 365 dispuesto en la Entidad.

g) Por último, con el fin de dar continuidad a la solución de protección de marca, adquirida en el año pasado, se requiere contratar la adquisición del licenciamiento por un año más,

permitiendo la visibilidad y monitoreo de DIMAR como marca y sus principales activos de información, en las diferentes capas de la internet, mitigando posibles ataques, suplantaciones o uso inadecuados del Nombre de la Entidad en la red."

Que en consideración de lo expuesto, el Grupo Intendencia Regional Central de la Dirección General Marítima, el día 02 de septiembre del 2026, efectuó publicación del estudio previo, aviso de convocatoria, proyecto de pliego de condiciones y demás documentos correspondientes al proceso de Selección Abreviada de Menor Cuantía No. **346-GINREDCE-2026,** cuyo objeto es la **"ADQUISICIÓN DEL LICENCIAMIENTO DE LAS HERRAMIENTAS DE SEGURIDAD, MONITOREO Y SERVICIOS PARA LA DIMAR, CONFORME CON LAS ESPECIFICACIONES ESTABLECIDAS EN EL ANEXO TÉCNICO",** hasta por la suma de **MIL DOSCIENTOS CUARENTA Y SEIS MILLONES TRESCIENTOS SESENTA Y SEIS MIL QUINIENTOS CUARENTA Y CINCO PESOS ($1.246.366.545,00)** incluido IVA (cuando aplique) y las demás erogaciones que correspondan, de acuerdo con el Certificado de Disponibilidad Presupuestal CDP ***No. 47126 del 30 de julio del 2026***

Que, dentro del lapso establecido para observar el proyecto de pliego de condiciones, es decir del 02 de septiembre de 2026 hasta el 09 de septiembre de 2026, se recibió observaciones de carácter técnico, así:



Que las observaciones fueron resueltas por los comités estructuradores, mediante Formulario de Preguntas y Respuestas publicado en la plataforma del SECOP II el 18 de septiembre de 2026.

Que como consta en acta levantada en la sesión del Comité de Adquisiciones del Grupo de Intendencia Regional Central de la Dirección General Marítima levantada el día 18 de septiembre de 2026, los miembros participantes del comité de adquisiciones y comités estructuradores sugeridos en estudio debatieron y en consideración del desarrollo del proceso de selección referido, recomendaron la apertura de este.

Que en cumplimiento a lo establecido en el artículo 2.2.1.2.4.2.2. concordante con el artículo 2.2.1.2.4.2.4 del Decreto 1082 de 2015, se tiene que el presente proceso **NO será limitado** a la participación de **MIPYMES**, teniendo en cuenta que no se recibió dentro del plazo establecido solicitudes de limitación **conforme al artículo 2.2.1.2.4.2.4** del Decreto 1082 de 2015; por lo que podrá participar abiertamente todas las empresas sin importar su tamaño empresarial.

Que persistiendo la necesidad Institucional de adelantar el proceso de **SELECCIÓN ABREVIADA MENOR CUANTÍA No. 346-GINREDCE-2026,** cuyo objeto es la **"ADQUISICIÓN DEL LICENCIAMIENTO DE LAS HERRAMIENTAS DE SEGURIDAD, MONITOREO Y SERVICIOS PARA LA DIMAR, CONFORME CON LAS ESPECIFICACIONES ESTABLECIDAS EN EL ANEXO TÉCNICO",** hasta por la suma de **MIL DOSCIENTOS CUARENTA Y SEIS MILLONES TRESCIENTOS SESENTA Y SEIS MIL QUINIENTOS CUARENTA Y CINCO PESOS ($1.246.366.545,00)** incluido IVA (cuando aplique) y las demás erogaciones que correspondan, de acuerdo con el Certificado de Disponibilidad Presupuestal CDP **No. 47126 del 30 de julio del 2026.**

Que, el Coordinador del Grupo Intendencia Regional Central de la Dirección General Marítima – DIMAR, previa consideración del desarrollo del mismo y concepto de sus Comités y órganos Asesores, estima pertinente dar apertura al proceso de **SELECCIÓN ABREVIADA MENOR CUANTÍA No. 346-GINREDCE-2026,** acuerdo los términos dispuestos en la normatividad que rige la materia.

Que en cumplimiento a lo establecido en el artículo 66 de la Ley 80 de 1993, la Ley 850 de 2003 y el Decreto 1082 del 26 de mayo de 2015, *POR MEDIO DEL CUAL SE EXPIDE EL DECRETO ÚNICO REGLAMENTARIO DEL SECTOR ADMINISTRATIVO DE PLANEACIÓN NACIONAL*, LIBRO 2 "*RÉGIMEN REGLAMENTARIO DEL SECTOR ADMINISTRATIVO DE PLANEACIÓN NACIONAL*", PARTE 2 "*REGLAMENTACIONES*", TITULO 1 "*CONTRATACION ESTATAL*", CAPITULO 1 "*SISTEMA DE COMPRAS Y CONTRATACION PUBLICA*", SECCION 2 "*ESTRUCTURA Y DOCUMENTOS DE PROCESO DE CONTRATACION*", SUBSECCION 1 "*PLANEACION*" articulo 2.2.1.1.2.1.5."*Acto administrativo de apertura del proceso de selección*", numeral 5, convocamos a las personas naturales y/o jurídicas, en forma individual y/o plural, nacional y/o foránea y en especial las Veedurías Ciudadanas para que en ejercicio control social, formulen lasrecomendaciones que consideren procedentes, que permitan garantizar la eficiencia Institucional y la probidad en la actuación de los funcionarios públicos que intervienen el presente proceso, coadyuvando en la selección objetiva del proponente que satisfaga de manera oportuna la necesidad Institucional.

Que, en virtud de lo expuesto, el Coordinador del Grupo Intendencia Regional Central de la Dirección General Marítima – DIMAR,

RESUELVE

ARTÍCULO PRIMERO: Ordenar la **APERTURA** del proceso de **SELECCIÓN ABREVIADA MENOR CUANTÍA No. 346-GINREDCE-2026,** cuyo objeto es la **"ADQUISICIÓN DEL LICENCIAMIENTO DE LAS HERRAMIENTAS DE SEGURIDAD, MONITOREO Y SERVICIOS PARA LA DIMAR, CONFORME CON LAS ESPECIFICACIONES ESTABLECIDAS EN EL ANEXO TÉCNICO",** hasta por la suma de **MIL DOSCIENTOS CUARENTA Y SEIS MILLONES TRESCIENTOS SESENTA Y SEIS MIL QUINIENTOS CUARENTA Y CINCO PESOS ($1.246.366.545,00)** incluido IVA (cuando aplique) y las demás erogaciones que correspondan, de acuerdo con el Certificado de Disponibilidad Presupuestal CDP ***No. 47126 del 30 de julio del 2026***

ARTÍCULO SEGUNDO: El proceso de **SELECCIÓN ABREVIADA MENOR CUANTÍA No. 346-GINREDCE-2026,** cuyo objeto es la **"ADQUISICIÓN DEL LICENCIAMIENTO DE LAS HERRAMIENTAS DE SEGURIDAD, MONITOREO Y SERVICIOS PARA LA DIMAR, CONFORME CON LAS ESPECIFICACIONES ESTABLECIDAS EN EL ANEXO TÉCNICO", NO se LIMITARÁ a MIPYME,** de conformidad con los argumentos expuestos en la parte considerativa de la presente resolución.

ARTÍCULO TERCERO: Informar que la apertura del presente proceso se hará a partir de la publicación del presente documento y los pliegos de condiciones definitivos en el portal Secop II.

Este proceso de contratación se regirá por el cronograma que aparece en la plataforma Secop II.

ARTÍCULO CUARTO: **ORDENAR** la Publicación de la presente Resolución y el Pliego de Condiciones Definitivo en el portal del Secop II.

ARTÍCULO QUINTO: La presente resolución rige a partir de su expedición.

PUBLÍQUESE Y CÚMPLASE.

Teniente de Fragata ERVIN NAZZIN VEGA OSPINA
Coordinador del Grupo de Intendencia Regional Central GINREDCE
Dirección General Marítima
Delegatario del Gasto