

MINISTERIO DE MEDIO AMBIENTE Y RECURSOS NATURALES

Dirección de Tecnología de la Información y Comunicación

**INFORME JUSTIFICATIVO
PARA LA CONTRATACIÓN DEL SERVICIO DE
COLOCATION EN CENTRO DE DATOS**

Entidad:	Ministerio de Medio Ambiente y Recursos Naturales (MIMARENA)
Área Solicitante:	Dirección de Tecnologías de la Información y Comunicaciones (DTIC)
Fecha:	Julio de 2026
Proceso:	<i>[Pendiente del número del proceso]</i>

TABLA DE CONTENIDO

○ 1. Antecedentes	3
○ 2. Marco Legal y Normativo	3
○ 3. Diagnóstico de la Situación Actual	5
○ 3.1 Infraestructura Eléctrica	5
○ 3.2 Análisis de Riesgos	6
○ 4. Justificación de la Necesidad	7
○ 5. Beneficios Institucionales de la Contratación	8
○ 5.1 Continuidad Operativa	8
○ 5.2 Mayor Disponibilidad de los Servicios	8
○ 5.3 Seguridad Física y Protección de Activos	8
○ 5.4 Reducción de Riesgos Operacionales	9
○ 5.5 Escalabilidad y Crecimiento Futuro	9
○ 5.6 Optimización de Recursos	9
○ 6. Justificación Técnica	10
○ 7. Justificación Económica	11
○ 8. Alineación Estratégica	12
○ 9. Conclusión	12

1. ANTECEDENTES

La transformación digital y la creciente dependencia de los sistemas tecnológicos institucionales han convertido la disponibilidad y seguridad de la infraestructura tecnológica en un elemento estratégico para el cumplimiento de las funciones del Ministerio de Medio Ambiente y Recursos Naturales.

Actualmente, los servicios tecnológicos soportan procesos críticos relacionados con la gestión administrativa, operativa y misional de la institución, incluyendo sistemas de información ambiental, plataformas de gestión de trámites, el Data Warehouse institucional, servicios de comunicación interna y externa, y aplicaciones de soporte a la toma de decisiones. La interrupción de estos servicios tendría un impacto directo en la capacidad del Ministerio para cumplir su mandato legal y constitucional de protección y gestión de los recursos naturales del país.

En virtud de lo anterior, y tras un diagnóstico técnico exhaustivo de las condiciones actuales de la infraestructura del centro de datos institucional, se ha identificado la necesidad imperiosa de contratar un servicio de Colocation en un Centro de Datos certificado Tier III o superior, que permita alojar la infraestructura tecnológica institucional en un entorno especializado, seguro, altamente disponible y alineado con las mejores prácticas internacionales para la operación de servicios críticos.

2. MARCO LEGAL Y NORMATIVO

La presente contratación se fundamenta en el siguiente marco legal y normativo vigente en la República Dominicana:

2.1 La Ley núm. 47-25 de Contrataciones Públicas, promulgada en julio de 2025, establece el marco jurídico que regula las contrataciones de bienes, servicios, obras y demás contrataciones realizadas por los órganos y entes sujetos a su ámbito de aplicación. Esta normativa tiene como finalidad garantizar la transparencia, eficiencia, igualdad de participación, libre competencia, sostenibilidad, integridad y el adecuado uso de los recursos públicos.

Asimismo, la Ley núm. 47-25 contempla determinadas situaciones que pueden ser tramitadas mediante procedimientos especiales o de excepción, incluyendo aquellas contrataciones donde exista un proveedor único o exclusividad debidamente justificada, siempre que se cumplan las condiciones, requisitos y procedimientos establecidos en la propia ley y su reglamento de aplicación, y que no se utilicen para evadir los principios que rigen el sistema de contrataciones públicas.

"Las contrataciones sustentadas en derechos de exclusividad o cuando los bienes o servicios solo puedan ser suministrados por un proveedor determinado deberán estar debidamente justificadas y realizarse conforme a los procedimientos previstos en la Ley núm. 47-25 y su Reglamento de Aplicación"

2.3 Normativas Técnicas

La contratación se alinea con las siguientes normativas y estándares técnicos aplicables:

- **NORTIC A7** – Norma sobre Seguridad de las Tecnologías de la Información y Comunicación en el Estado Dominicano, emitida por la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC).
- **NORTIC A5** – Norma para la Prestación y Uso de Servicios en la Nube (Cloud Computing) para el Estado dominicano.
- **ISO/IEC 27001** – Sistema de Gestión de Seguridad de la Información, estándar internacional para la protección de activos de información.
- **ANSI/TIA-942** – Estándar de infraestructura de telecomunicaciones para centros de datos, que define los niveles de clasificación (Tier I a IV).
- **Uptime Institute Tier III** – Estándar de diseño y construcción para centros de datos con mantenimiento concurrente y disponibilidad de 99.982%.
- **PCI DSS** – Estándar de seguridad de datos para la industria de tarjetas de pago, aplicable a la protección de información sensible.

2.4 Marco Constitucional

La Constitución de la República Dominicana, proclamada el 27 de octubre de 2024, establece en sus disposiciones el deber del Estado de proteger los recursos naturales y promover el desarrollo sostenible. El Ministerio de Medio Ambiente y Recursos Naturales, como entidad rectora en materia ambiental, requiere de una infraestructura tecnológica robusta y confiable para el cumplimiento efectivo de este mandato constitucional.

3. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

Como parte del Plan Operativo Anual 2026 (producto DTIC.06 – Plan de mejora de infraestructura documentado), la Dirección de Tecnología de la Información y Comunicación realizó un diagnóstico integral de la infraestructura del centro de datos institucional. Los hallazgos revelan condiciones que comprometen la continuidad operativa y la seguridad de los activos tecnológicos del Ministerio.

3.1 Infraestructura Eléctrica – Riesgo ALTO

El diagnóstico técnico del Data Center institucional identificó la infraestructura eléctrica como el riesgo de mayor criticidad, clasificado como ALTO. Las principales deficiencias identificadas son:

- **Acometida eléctrica única:** El centro de datos actual depende de una sola acometida eléctrica comercial, sin redundancia. Cualquier falla en el suministro eléctrico provoca una interrupción total de los servicios tecnológicos.
- **Sistema UPS sin redundancia:** El sistema de alimentación ininterrumpida (UPS) no cuenta con configuración redundante (N+1 o 2N). Una falla en el UPS deja la infraestructura sin protección ante fluctuaciones o cortes eléctricos.
- **Generador de emergencia limitado:** La capacidad del generador de emergencia existente es insuficiente para sostener la operación completa del centro de datos durante cortes prolongados, con un tiempo de autonomía significativamente inferior a las 14 horas mínimas recomendadas por estándares internacionales.
- **Ausencia de monitoreo eléctrico continuo:** No se cuenta con sistemas de monitoreo y control en tiempo real para los circuitos eléctricos, lo que impide la detección temprana de anomalías y la respuesta proactiva ante incidentes.
- **Cableado eléctrico obsoleto:** Parte del cableado eléctrico del centro de datos no cumple con los estándares actuales de seguridad y capacidad, incrementando el riesgo de fallas eléctricas, sobrecalentamiento e incluso incendios.
- **Climatización comprometida:** Los sistemas de climatización del espacio actual no cuentan con la redundancia ni la precisión requeridas para un entorno de misión crítica. Las fluctuaciones de temperatura ponen en riesgo la vida útil y el rendimiento de los equipos.

Estas condiciones representan un riesgo inaceptable para la operación continua de los servicios tecnológicos institucionales. Un evento eléctrico mayor —como los que se han registrado en múltiples ocasiones durante temporadas de huracanes y tormentas— podría resultar en la pérdida total de servicios por períodos prolongados, con consecuencias directas sobre la gestión ambiental nacional.

3.2 Análisis de Riesgos

A continuación se presenta la matriz de riesgos identificados en la infraestructura actual del centro de datos institucional:

Riesgo Identificado	Probabilidad	Impacto	Consecuencia
Falla eléctrica por acometida única	ALTA	CRÍTICO	Interrupción total de servicios tecnológicos. Pérdida de disponibilidad de sistemas críticos (Data Warehouse, gestión de trámites, Línea Verde).
Falla del sistema UPS sin redundancia	MEDIA	CRÍTICO	Equipos expuestos a picos de tensión, fluctuaciones y cortes. Riesgo de daño físico a servidores y pérdida de datos.
Generador con autonomía insuficiente	MEDIA	ALTO	Incapacidad de sostener operaciones durante cortes prolongados (huracanes, tormentas). Indisponibilidad extendida.
Climatización sin redundancia	MEDIA	ALTO	Sobrecalentamiento de equipos, reducción de vida útil, apagados de emergencia por temperatura.
Cableado eléctrico obsoleto	MEDIA	CRÍTICO	Riesgo de cortocircuitos, sobrecalentamiento e incendio en sala de servidores. Pérdida total de infraestructura.

El análisis de riesgos demuestra que la infraestructura eléctrica actual del centro de datos institucional presenta vulnerabilidades críticas que no pueden ser mitigadas mediante mejoras parciales. La solución integral requiere el traslado de la infraestructura tecnológica a un entorno diseñado y certificado para la operación de sistemas de misión crítica.

4. JUSTIFICACIÓN DE LA NECESIDAD

La contratación del servicio de Colocation en un Centro de Datos responde a la necesidad institucional de disponer de una infraestructura tecnológica especializada que garantice la operación continua, segura y eficiente de los sistemas de información y servicios digitales del Ministerio de Medio Ambiente y Recursos Naturales.

Asimismo, la presente contratación se encuentra alineada con los objetivos institucionales de fortalecimiento tecnológico, modernización de la infraestructura digital y continuidad operativa, contribuyendo a garantizar la disponibilidad, integridad y confiabilidad de los servicios tecnológicos que soportan los procesos sustantivos, administrativos y estratégicos del Ministerio.

La colocación de la infraestructura tecnológica institucional en un centro de datos especializado permite disponer de un entorno diseñado específicamente para alojar plataformas de misión crítica, proporcionando niveles de seguridad, redundancia, disponibilidad y resiliencia superiores a los que pueden ofrecer las instalaciones actuales del Ministerio. Esta modalidad garantiza que los activos tecnológicos institucionales operen bajo estándares internacionales, con capacidades adecuadas de protección física y lógica, continuidad energética, climatización especializada y conectividad de alta disponibilidad.

Asimismo, la infraestructura deberá encontrarse ubicada en instalaciones diseñadas para mitigar riesgos asociados a fenómenos naturales y contingencias mayores, garantizando la continuidad de las operaciones institucionales ante eventos adversos, en concordancia con los requerimientos de resiliencia y disponibilidad establecidos para infraestructuras de misión crítica.

Para satisfacer las necesidades operativas y de continuidad del negocio de la institución, la infraestructura requerida debe ofrecer:

- **Disponibilidad permanente de energía eléctrica** mediante esquemas de redundancia 2N+1, con mínimo dos acometidas eléctricas independientes y al menos cinco generadores de emergencia.
- **Sistemas de climatización de precisión** totalmente redundantes para la conservación adecuada de los equipos tecnológicos, con organización Hot Aisle / Cold Aisle.
- **Conectividad de alta disponibilidad** mediante condición de Network Access Point (NAP) neutral, con acceso a un mínimo de catorce proveedores de telecomunicaciones y cinco niveles de redundancia.
- **Seguridad física y lógica de nivel empresarial**, incluyendo controles biométricos de acceso, vigilancia 24/7, y Centro de Operaciones de Seguridad (SOC).
- **Monitoreo y soporte técnico especializado** veinticuatro (24) horas al día, siete (7) días a la semana, durante todo el año, con Network Operation Center (NOC) y servicios de manos remotas e inteligentes.
- **Condiciones de operación alineadas con estándares internacionales** Tier III (Uptime Institute), ISO/IEC 27001, PCI DSS y SOC (AICPA).

La permanencia de los equipos tecnológicos en las instalaciones actuales, que no cuentan con estos niveles de robustez —como ha sido demostrado en el diagnóstico de la sección anterior—, incrementa significativamente el riesgo de interrupción de los servicios institucionales,

indisponibilidad de plataformas críticas, afectación a los procesos operativos, pérdida de información y posibles impactos en la prestación de los servicios ofrecidos por el Ministerio a la ciudadanía.

5. BENEFICIOS INSTITUCIONALES DE LA CONTRATACIÓN

5.1 Continuidad Operativa

El servicio permitirá garantizar la operación ininterrumpida de las plataformas tecnológicas institucionales mediante infraestructura diseñada para soportar eventos eléctricos, fallos de climatización y contingencias operativas. El centro de datos deberá contar con múltiples acometidas eléctricas, sistemas UPS redundantes en configuración 2N+1 y generadores de emergencia con autonomía mínima de catorce (14) horas que aseguren la continuidad del servicio, eliminando las vulnerabilidades críticas identificadas en el diagnóstico actual.

5.2 Mayor Disponibilidad de los Servicios

La solución exige un nivel de disponibilidad de hasta 99.999% para la plataforma integral, reduciendo significativamente la probabilidad de interrupciones que puedan afectar los servicios tecnológicos prestados a usuarios internos y externos. Esto representa una mejora sustancial respecto a las condiciones actuales, donde la infraestructura eléctrica de acometida única hace imposible garantizar estos niveles de disponibilidad.

Parámetro	Nivel Mínimo Requerido
Disponibilidad de energía AC	99.99%
Estabilidad de humedad relativa	99.99% (55% ± 5%)
Estabilidad de temperatura	99.99% (máx. 27°C / 81°F)
Monitoreo de red	24 x 7, respuesta ≤ 30 min
Disponibilidad SLA global	≥ 99.999%

5.3 Seguridad Física y Protección de los Activos Tecnológicos

El centro de datos deberá disponer de controles estrictos de acceso biométrico/electrónico, monitoreo permanente, vigilancia privada con equipos de detección de metales, rondas de supervisión con emisión de reportes, sistemas de detección y respuesta ante incidentes de seguridad, así como mecanismos de protección contra incendios y desastres. Estas condiciones fortalecen significativamente la protección de los activos tecnológicos institucionales respecto a las condiciones actuales.

5.4 Reducción de Riesgos Operacionales

La infraestructura propuesta está diseñada para resistir fenómenos naturales (huracanes, terremotos), interrupciones eléctricas, fallos de conectividad y otras eventualidades que puedan comprometer la continuidad operativa de la institución. Las instalaciones deberán ubicarse fuera de zonas de riesgo de inundación/tsunami, con elevación mínima de 46 pies sobre el nivel del mar, y construidas conforme a códigos civiles de categoría A o superior.

5.5 Escalabilidad y Crecimiento Futuro

La contratación permitirá disponer de una plataforma preparada para el crecimiento de la infraestructura tecnológica institucional, mediante espacios de expansión, servicios complementarios y facilidades para futuras adecuaciones sin incurrir en nuevas inversiones de infraestructura física. La disponibilidad de cross-connect dentro del propio centro de datos facilitará la incorporación de nuevos servicios de telecomunicaciones y enlaces dedicados.

5.6 Optimización de Recursos

La utilización de un centro de datos especializado evita que la institución tenga que realizar inversiones significativas en construcción, adecuación, certificación, mantenimiento y operación de instalaciones propias con estándares Tier III, permitiendo concentrar los recursos en sus actividades sustantivas de protección ambiental y gestión de recursos naturales.

6. JUSTIFICACIÓN TÉCNICA

Las especificaciones técnicas definidas para el proceso responden a requerimientos de misión crítica y se fundamentan en estándares internacionales para centros de datos. Los requerimientos técnicos mínimos han sido definidos en la Ficha Técnica del servicio y se resumen a continuación:

6.1 Infraestructura Física

- Instalación con área mínima de 20,000 pies cuadrados.
- Ubicación fuera de zona de riesgo de inundación/tsunami, con elevación mínima de 46 pies sobre el nivel del mar.
- Gabinete estándar de 42U con puertas frontal y trasera con cerradura, compatible con PCI DSS.
- Estructura construida para resistir huracanes, terremotos y ataques, conforme a códigos civiles categoría A o superior.

6.2 Energía

- Infraestructura eléctrica en configuración de redundancia 2N+1.
- Mínimo dos (2) acometidas eléctricas independientes.
- Mínimo cinco (5) generadores de emergencia con autonomía de al menos 14 horas.
- Sistemas UPS redundantes de alta generación.
- Circuito de energía redundante 208V AC (A+B) con sistema de monitoreo y control.

6.3 Conectividad

- Condición de Network Access Point (NAP) neutral, con acceso a un mínimo de catorce (14) proveedores de telecomunicaciones.
- Servicio de Internet gestionado (Managed Router Service) con mínimo cinco (5) niveles de redundancia.
- Disponibilidad de cross-connect (fibra óptica y cobre) dentro del propio centro de datos.
- Soporte de enlaces dedicados punto a punto, MPLS e internacionales.

6.4 Seguridad y Monitoreo

- Seguridad física perimetral con vigilancia privada 24/7, controles biométricos de acceso y equipos de detección de metales.
- Centro de Operaciones de Seguridad (SOC) con monitoreo, detección y gestión de incidentes de ciberseguridad.
- Network Operation Center (NOC) con monitoreo 24x7x365 de redes, sistemas y equipos.

- Soporte técnico en sitio y remoto (niveles 1, 2 y 3) disponible 24/7, con servicios de manos remotas e inteligentes.
- Mesa de ayuda (Help Desk) operativa 24/7/365 con herramienta de gestión de tickets.

6.5 Certificaciones Requeridas

- Tier III Design/Facility (Uptime Institute) o equivalente ANSI/TIA-942 Rated 3.
- ISO/IEC 27001 (Gestión de Seguridad de la Información).
- PCI DSS (según aplique al espacio de colocación).
- SOC (Service Organization Control), tipo AICPA SOC o equivalente.
- TIA 942.

Estas características son indispensables para garantizar niveles adecuados de disponibilidad, rendimiento, seguridad y resiliencia tecnológica, y responden directamente a las vulnerabilidades críticas identificadas en el diagnóstico del centro de datos actual.

7. JUSTIFICACIÓN ECONÓMICA

Desde el punto de vista económico, la contratación del servicio de Colocation representa una alternativa significativamente más eficiente y sostenible que la construcción o adecuación de una instalación propia con características equivalentes.

La implementación de un centro de datos institucional con certificación Tier III implicaría inversiones considerables en los siguientes rubros:

Rubro de Inversión	Característica
Infraestructura civil especializada	Construcción de edificación categoría A con protección sísmica, anti-huracanes y elevación mínima de 46 pies SNM
Sistemas eléctricos redundantes 2N+1	Dos acometidas eléctricas independientes, tableros de distribución, transferencia automática
Generadores de emergencia	Mínimo 5 generadores con 14+ horas de autonomía, tanques de combustible, sistemas de distribución
Sistemas UPS industriales	UPS redundantes de alta generación en configuración 2N+1
Climatización de precisión	Unidades redundantes, organización Hot Aisle/Cold Aisle, monitoreo ambiental continuo
Seguridad física especializada	Control biométrico, CCTV, detección de metales, vigilancia 24/7, sistema contra incendios
Personal técnico permanente (NOC)	Equipo técnico 24x7x365 niveles 1, 2 y 3 para monitoreo y soporte
Conectividad multiproveedor (NAP)	Infraestructura para 14+ proveedores de telecomunicaciones con redundancia
Certificaciones y auditorías	Tier III, ISO 27001, PCI DSS, SOC — procesos de certificación y auditorías anuales
Mantenimiento preventivo y correctivo	Mantenimiento continuo de toda la infraestructura electromecánica y de seguridad

El costo estimado de construcción y equipamiento de un centro de datos Tier III propio, con las características técnicas requeridas, supera ampliamente la inversión necesaria para la contratación del servicio de colocation por el período establecido. Adicionalmente, el modelo de colocation elimina los costos recurrentes de mantenimiento, personal especializado, renovación de certificaciones y actualización de infraestructura, que recaen sobre el proveedor del servicio.

Mediante la contratación del servicio, la institución accede a una infraestructura ya certificada y operativa, reduciendo significativamente los costos de inversión inicial (CAPEX) y convirtiendo el

gasto en un modelo operativo (OPEX) predecible y presupuestable, garantizando el acceso inmediato a capacidades tecnológicas de clase mundial.

8. ALINEACIÓN ESTRATÉGICA

La contratación del servicio de Colocation se alinea directamente con los siguientes instrumentos de planificación institucional y nacional:

- **Plan Operativo Anual (POA) 2026:** Producto DTIC.06 – Plan de mejora de infraestructura documentado, que identifica la evaluación de colocation como uno de los cuatro ejes de mejora prioritarios para la infraestructura tecnológica del Ministerio.
- **Estrategia Nacional de Transformación Digital:** La modernización de la infraestructura tecnológica del Estado dominicano requiere que las entidades gubernamentales adopten estándares internacionales de disponibilidad y seguridad para sus plataformas de misión crítica.
- **Plan Estratégico Institucional:** El fortalecimiento de la capacidad tecnológica del Ministerio es un habilitador transversal para el cumplimiento de los objetivos misionales de protección ambiental, gestión de recursos naturales y desarrollo sostenible.

9. CONCLUSIÓN

Luego de evaluar los requerimientos tecnológicos, operativos, de seguridad y de continuidad del negocio del Ministerio de Medio Ambiente y Recursos Naturales, y considerando los hallazgos del diagnóstico técnico que revelan vulnerabilidades críticas en la infraestructura eléctrica del centro de datos actual —clasificadas como riesgo ALTO—, se concluye que la contratación del servicio de Colocation en un Centro de Datos certificado Tier III o superior resulta necesaria, conveniente y estratégicamente justificada para garantizar la operación segura, eficiente e ininterrumpida de la infraestructura tecnológica institucional.

La solución propuesta permitirá:

- Fortalecer la disponibilidad de los sistemas y servicios institucionales, alcanzando niveles de SLA de 99.999%.
- Eliminar las vulnerabilidades críticas de la infraestructura eléctrica actual mediante redundancia 2N+1.
- Incrementar los niveles de seguridad de la información conforme a estándares ISO 27001 y PCI DSS.
- Reducir los riesgos operativos y tecnológicos asociados a fenómenos naturales y contingencias.
- Asegurar la continuidad de las operaciones críticas ante cualquier eventualidad.
- Optimizar el uso de los recursos institucionales al evitar inversiones de infraestructura civil y certificaciones propias.
- Cumplir con las normativas y estándares nacionales (NORTICs) e internacionales aplicables.

Esta contratación contribuirá al fortalecimiento de la resiliencia tecnológica institucional, proporcionando una plataforma robusta, escalable y altamente disponible, capaz de respaldar las iniciativas de transformación digital y las necesidades actuales y futuras del Ministerio de Medio Ambiente y Recursos Naturales.

La presente contratación se considera indispensable para garantizar la continuidad de los servicios tecnológicos institucionales y mantener los niveles de disponibilidad, seguridad y confiabilidad requeridos para la operación de las plataformas críticas del Ministerio. En consecuencia, se recomienda la aprobación y continuidad del proceso de contratación del servicio de Colocation en Centro de Datos, conforme a las especificaciones técnicas definidas en la Ficha Técnica y los Términos de Referencia elaborados por la Dirección de Tecnología de la Información y Comunicación (DTIC).

Atentamente,

Nivel	Nombre y Posición	Firma	Fecha	Sello
Elaborado por	Carlos Gómez Mallol Encargado Departamento de Operaciones TIC			
Aprobado Final	Raymer D. Ortiz Drullard Director de Tecnología de la Información y Comunicación			