Superintendencia del Mercado de Valores
de la República Dominicana

ESPECIFICACIONES TÉCNICAS

CONTRATACIÓN DE SERVICIOS PARA LA IMPLEMENTACIÓN DEL SISTEMA INSTITUCIONAL DE CLASIFICACIÓN DE LA INFORMACIÓN (TLP) Y CONTROLES DE DATA LOSS PREVENTION (DLP) PARA LA SIMV.

REFERENCIA: SIV-CCC-CP-2026-0005

Santo Domingo de Guzmán
23 de marzo del 2026

CONTENIDO

1. NOMBRE DEL PROCESO 3
2. OBJETIVO GENERAL 3
3. OBJETIVO DEL DOCUMENTO 3
4. CONOCIMIENTO Y ACEPTACION DEL PRESENTE DOCUMENTO 3
5. IDIOMA 3
6. ÓRGANO RESPONSABLE DEL PROCESO. 3
7. FUENTE DE LOS RECURSOS 4
8. LUGAR DE PRESTACIÓN DE LOS SERVICIOS 4
9. TIEMPO DE EJECUCIÓN DE LOS SERVICIOS 4
10. CONDICIONES DE PAGO Y FACTURACIÓN 4
11. SERVICIO A REQUERIR 5
12. OTROS REQUERIMIENTOS 9
13. ENTREGABLES 10

13.1 Componente de Gobernanza 10

13.2 Componente de Concientización 11

13.3 Componente Técnico 11

13.4 Componente Integración y Control 11

14. SUBSANACIONES 12
15. CRITERIO DE EVALUACIÓN TÉCNICA Y ECONÓMICA 12
16. CRITERIO DE ADJUDICACIÓN 14
17. VIGENCIA DEL CONTRATO 14
18. PLAZO PARA LA SUSCRIPCIÓN DEL CONTRATO 15
19. OBLIGACIONES DEL PROVEEDOR 15
20. PROPIEDAD INTELECTUAL 15
21. CONTACTOS. 16
22. FORMULARIOS TIPO. 16

1. NOMBRE DEL PROCESO

Contratación de servicios para la implementación del Sistema Institucional de Clasificación de la Información (TLP) y controles de Data Loss Prevention (DLP) para la SIMV.

2. OBJETIVO GENERAL

Contratar un servicio especializado para el diseño, formalización e implementación del Sistema Institucional de Clasificación y Protección de la Información, basado en el Traffic Light Protocol (TLP), y la configuración de controles de Data Loss Prevention (DLP), conforme al Proyecto "Integridad de la Información y Clasificación de los Accesos (Rojo, Ámbar y Verde)" que permita fortalecer la gobernanza, el control de accesos, la prevención de fuga de información y la generación de evidencia trazable para fines de auditoría y cumplimiento normativo.

3. OBJETIVO DEL DOCUMENTO

El objetivo del presente documento es establecer el conjunto de cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, por el que se fijan los requisitos, exigencias, facultades, derechos y obligaciones de las personas naturales o jurídicas, nacionales o extranjeras que deseen participar en el presente procedimiento.

Este documento constituye la base para la preparación de las Ofertas. Si el Oferente/Proponente omite suministrar alguna parte de la información requerida en el presente documento de Especificaciones Técnicas o presenta una información que no se ajuste sustancialmente en todos sus aspectos al mismo, el riesgo estará a su cargo y el resultado podrá ser el rechazo de su propuesta.

4. CONOCIMIENTO Y ACEPTACION DEL PRESENTE DOCUMENTO

El sólo hecho de un Oferente/Proponente participar en el presente procedimiento implica pleno conocimiento, aceptación y sometimiento por él, por sus miembros, ejecutivos, y su Representante Legal, a los procedimientos, condiciones, estipulaciones y normativas, sin excepción alguna, establecidos en las presentes Especificaciones Técnicas, el cual tienen carácter jurídicamente obligatorio y vinculante.

5. IDIOMA

El idioma oficial del presente proceso es el español, por tanto, toda la correspondencia y documentos generados durante el procedimiento que intercambien los oferentes y el Comité de Contrataciones Públicas deberán ser presentados en este idioma o de encontrarse en idioma distinto, deberán de contar con la traducción al español realizada por un intérprete judicial debidamente autorizado.

6. ÓRGANO RESPONSABLE DEL PROCESO.

El Órgano responsable del presente proceso es el Comité de Contrataciones Públicas. El Comité de

Contrataciones Públicas está integrado por cinco (5) miembros:

- El funcionario de mayor jerarquía de la institución, o quien este designe, quien lo presidirá;
- La Directora Administrativa y Financiera de la entidad;
- La Directora Jurídica de la entidad, quien actuará en calidad de Asesor Legal;
- El Director de Planificación y Desarrollo;
- La Encargada de la Oficina de Libre Acceso a la Información.

7. FUENTE DE LOS RECURSOS

La Superintendencia del Mercado de Valores de la República Dominicana, de conformidad con el artículo 93 de la Ley núm. 47-25 sobre Contrataciones Públicas, de fecha veintiocho (28) de julio del año dos mil veinticinco (2025), ha tomado las medidas previsoras necesarias a los fines de garantizar la apropiación de fondos correspondiente, dentro del Presupuesto del año 2026, que sustentará el pago para la presente contratación.

8. LUGAR DE PRESTACIÓN DE LOS SERVICIOS

Todos los servicios deberán ser prestados en la Superintendencia del Mercado de Valores de la República Dominicana, ubicada en la calle César Nicolás Penson, núm. 66, del sector Gascue, Santo Domingo de Guzmán.

9. TIEMPO DE EJECUCIÓN DE LOS SERVICIOS

El tiempo de ejecución de los servicios contratados serán ejecutados en un plazo máximo de 14 meses, contados a partir de la certificación del contrato ante la Contraloría General de la República.

Los servicios deberán ser ejecutados de la siguiente manera:

- Los servicios requeridos en el punto 11 del presente documento en un plazo no mayor a los ocho (8) meses, y;
- 6 meses de soporte post implementación, contados a partir de la recepción formal de los servicios requeridos.

10. CONDICIONES DE PAGO Y FACTURACIÓN

La forma de pago aplicable al presente procedimiento es la siguiente:

1. **Un primer pago del 20%** del monto total del contrato, correspondiente al pago del anticipo, en un plazo no mayor a treinta (30) días luego de la certificación del contrato ante la Contraloría General de la República y contra presentación de una Garantía del Buen Uso del Anticipo, mediante una Póliza de Fianza emitida por una compañía aseguradora en la República Dominicana, que cubra la totalidad

del avance. En caso de que el adjudicatario sea una Mipymes, se realizará un primer pago de un 30% correspondiente al pago de anticipo, luego de la certificación del contrato ante la Contraloría General de la República, conforme a lo establecido en el artículo 174 de la Ley núm. 47-25 de Contrataciones Públicas.

2. **Un segundo pago del 25%** del monto total del contrato, con impuestos incluidos, en un plazo no mayor a treinta (30) días luego de la presentación y aprobación de los entregables del numeral **13.1 Componente de Gobernanza** del documento de Especificaciones Técnicas. En caso de que el adjudicatario sea una Mipymes, el segundo pago se realizará por la suma del 15% del monto total del contrato.

3. **Un tercer pago del 15%** del monto total del contrato, con impuestos incluidos, en un plazo no mayor a treinta (30) días luego de la presentación y aprobación de los entregables del numeral **13.2 Componente Concientización** del documento de Especificaciones Técnicas.

4. **Un cuarto pago del 20%** del monto total del contrato, con impuestos incluidos, en un plazo no mayor a treinta (30) días luego de la presentación y aprobación de los entregables del numeral **13.3 Componente Técnico** del documento de Especificaciones Técnicas.

5. **Un pago final del 20%** del monto total del contrato, con impuestos incluidos, en un plazo no mayor a treinta (30) días luego de la presentación y aprobación de los entregables del numeral **13.4 Componente Integración y Control** del documento de Especificaciones Técnicas y el cierre formal del proyecto.

Los pagos se realizarán contra presentación en físico de factura original, debidamente firmada y sellada de acuerdo con los servicios recibidos, con crédito a treinta (30) días contados a partir de la emisión de las facturas. Las facturas deben ser emitida con NFC gubernamental, con impuestos incluidos aplicables, a beneficio de la Superintendencia del Mercado de Valores de la República Dominicana, RNC núm. 401-51572-5.

11. SERVICIO A REQUERIR

10.1. Alcance del Servicio

El servicio comprende la implementación integral de un modelo institucional de clasificación y protección de la información, que incluya:

- Formalización del marco de gobernanza de la información.
- Sensibilización y acompañamiento a los responsables de procesos y dueños de información.
- Implementación de mecanismos automáticos de clasificación y etiquetado.
- Configuración y alineación de controles tecnológicos para la prevención de fuga de información.
- Habilitación de capacidades de monitoreo, trazabilidad y generación de reportes.

El servicio deberá garantizar coherencia entre la clasificación definida, los accesos otorgados y los controles aplicados sobre la información institucional.

10.2. Gobernanza y Marco Normativo

El proveedor deberá entregar, como mínimo:

Política de Clasificación de la Información

- Alineada formalmente con: ISO/IEC 27001, NIST SP 800-53, GRDP y NORTIC A7
- Definición de niveles TLP: Rojo, Ámbar y Verde.
- Relación explícita entre clasificación y controles DLP
- Criterios técnicos y funcionales por nivel.
- Definición de restricciones por nivel:
    - Acceso
    - Envío externo
    - Copia a medios removibles
    - Impresión
    - Compartición

Procedimientos Operativos

- Procedimiento de clasificación inicial.
- Procedimiento de revisión periódica.
- Procedimiento de cambio de clasificación.
- Procedimiento de gestión de excepciones.
- Procedimiento de gestión de incidentes asociados a mala clasificación.

Definición Formal de Roles

Deberá diseñar y documentar:

- Rol de Data Owner.
- Rol de Data Custodian.
- Rol de Administrador Técnico.
- Rol de Seguridad de la Información.

Matriz RACI

Se deberá elaborar una matriz RACI formal que contemple:

- Clasificación.
- Validación.
- Autorización de accesos.
- Revisión periódica.
- Gestión de incidentes DLP.

10.3. Concientización y Adopción

Como parte del proceso de adopción a las actividades diarias, de los empleados, colaboradores y partes interesadas de la SIMV, el proveedor deberá diseñar e impartir un programa de concientización, estructurado por nivel:

Alta Dirección

- Sesión ejecutiva presencial sobre:
  - Riesgos regulatorios.
  - Impacto reputacional.
  - Responsabilidad institucional.
  - Modelo TLP.

Mandos Medios

- Talleres prácticos, virtual y/o presencial, sobre:
  - Rol como Data Owner.
  - Validación de clasificación.
  - Responsabilidad en autorizaciones.

Colaboradores con acceso a información

- Capacitación operativa, virtual, sobre:
  - Uso correcto de etiquetas.
  - Restricciones por nivel.
  - Consecuencias de mala clasificación.
  - Casos prácticos.

Se deberá entregar el material didáctico cediendo los derechos de uso y modificación a la SIMV, y evidencia de participación.

10.4. Implementación Técnica

La SIMV cuenta, en la suite de productos Microsoft 365, con la herramienta Purview, por lo que el proveedor deberá:

Implementación Microsoft Purview

- Configurar Sensitivity Labels alineadas al modelo TLP.
- Configurar políticas de auto-etiquetado.
- Configurar políticas DLP en:
  - Exchange Online.
  - SharePoint / OneDrive / Teams (si aplica).
- Configurar reportes de clasificación.

Implementación de Microsoft Purview Information Protection Scanner (On-Premise)

Requisito obligatorio:

- Instalación y configuración del Scanner en infraestructura institucional.
- Integración con el almacenamiento empresarial centralizado.
- Configuración de escaneo por fases.
- Definición de reglas de clasificación automática.

- Aplicación automática de etiquetas persistentes.
- Configuración de modo simulación y modo enforcement.
- Plan de escaneo progresivo del repositorio institucional.

Configuración de Controles DLP

El proveedor deberá configurar controles alineados a TLP en:

- Exchange Online.
- Microsoft Defender for Endpoint.
- Firewall / UTM (acompañamiento técnico).
- Gateway de correo Trend Micro (acompañamiento técnico).

Los controles deberán permitir:

- Detección.
- Alertamiento.
- Bloqueo automático según nivel Rojo / Ámbar.
- Generación de evidencia trazable.

Transferencia de Conocimiento

El proveedor deberá:

- Entregar documentación técnica completa.
- Realizar sesión formal de transferencia.
- Entregar manual operativo.
- Capacitar al equipo técnico interno en administración del Scanner y políticas DLP.

1.5. Monitoreo y Reportes

- Reporte de % de información clasificada.
- Distribución por nivel TLP.
- Reporte de eventos DLP detectados/bloqueados.
- Reporte de intentos de exfiltración.
- Evidencia exportable para auditoría.

1.6. Soporte y servicio post Implementación

El proveedor deberá garantizar un período de soporte técnico posterior a la finalización formal del proyecto, por un plazo no menor a seis (6) meses, contados a partir de la emisión del acta de cierre técnico. Durante dicho período, el soporte deberá incluir como mínimo:

- Ajustes finos de reglas de clasificación y políticas DLP.
- Corrección de configuraciones derivadas de errores u omisiones en la implementación.
- Asistencia técnica ante incidentes relacionados con la solución implementada.
- Orientación técnica al equipo interno sobre operación de la solución.

El soporte deberá brindarse bajo modalidad remota, dentro del horario laboral institucional, con tiempos de respuesta máximos definidos según criticidad.

12. OTROS REQUERIMIENTOS

Adicionalmente y de manera obligatoria, el oferente debe presentar en su oferta técnica lo siguiente:

a) **Experiencia del Oferente**. Deberá presentar contrato y/o orden de compra que acredite al menos un (1) proyecto en los últimos cinco (5) años relacionados con seguridad de la información, gobierno de datos, implementación de DLP o soluciones de protección de información, que incluyan los siguientes componentes:
   - Implementación de modelos de clasificación de información.
   - Implementación de mecanismos de clasificación automática y etiquetado.
   - Configuración de políticas de Data Loss Prevention (DLP).
   - Proyectos en entornos híbridos (cloud y on-premise).
   - Clasificación de información no estructurada.

b) **Perfil y Competencias del Equipo Técnico**. El personal propuesto deberá estar disponible durante toda la ejecución del proyecto. Cualquier sustitución deberá ser comunicada previamente a la SIMV y el recurso sustituto deberá contar con un perfil profesional equivalente o superior.

   El oferente deberá presentar los perfiles profesionales del equipo técnico mínimo requerido, con experiencia demostrable mediante la presentación de perfiles de proyectos y/o contratos de servicios similares. Este equipo será asignado al proyecto y estará compuesto por los siguientes profesionales:

   - **Un Gerente de Proyecto**:
     - Certificación vigente PMP (Project Management Professional) o certificación equivalente en peso en gestión de proyectos reconocida internacionalmente. No se considerarán válidas certificaciones emitidas por plataformas de autoformación sin acreditación internacional formal en gestión de proyectos.
     - Participación en al menos dos (2) proyectos de implementación tecnológica de complejidad similar o mayor.
     - Demostrar experiencia en conducción de talleres, sesiones ejecutivas o actividades de sensibilización relacionadas con seguridad de la información o gobierno de datos.

   - **Un especialista en Microsoft Information Protection:**
     - Profesional con certificación vigente, Microsoft SC-400 (Information Protection Administrator), y/o Microsoft SC-100 (Cybersecurity Architect), o certificación técnica equivalente en seguridad Microsoft.
     - Experiencia demostrable de proyectos relacionados con seguridad y gobernanza de datos en entornos Microsoft Azure y/o híbridos (cloud y on-premise), que hayan

incluido gobierno de datos, implementación de mecanismos de protección de información y/o controles de prevención de fuga de información.

- **Un Técnico en Seguridad,** mínimo 2 años de experiencia demostrable en**:**
    - Participación en al menos un proyecto de integración de controles de seguridad en entornos Microsoft 365 o híbridos.
    - Configuración y administración de FortiGate UTM o soluciones equivalentes.
    - Implementación de DLP en Microsoft Defender for Endpoint y Exchange Online.
    - Integración de controles de red y endpoint con clasificación de información.
    - Se valorará experiencia en entornos híbridos (cloud + on-premise).

c) Certificación ISO/IEC 27001. El oferente deberá acreditar que cuenta con certificación ISO/IEC 27001 vigente, emitido por un organismo certificador reconocido internacionalmente. Dicha certificación deberá encontrarse vigente durante todo el período de ejecución del servicio y cubrir, dentro de su alcance, las actividades de prestación de servicios de tecnología y seguridad de la información. En caso de vencimiento durante la ejecución del contrato adjudicado, deberá presentar un documento firmado y sellado, comprometiéndose a renovar y presentar dicha certificación en un plazo no mayor a 45 días calendarios, posterior a la fecha de vencimiento.

d) Confidencialidad y Protección de la Información. El oferente deberá garantizar, mediante documento firmado y sellado, la confidencialidad y no divulgación de información sensible, confidencial o reservada, a la que tenga acceso durante la ejecución del servicio.

13. ENTREGABLES

El proveedor deberá entregar, como mínimo, los siguientes productos documentales y técnicos:

13.1 Componente de Gobernanza

a) Documento formal de la **Política de Clasificación de la Información**, alineado con:
- ISO/IEC 27001:2022
- NIST SP 800-53 Rev. 5
- GDRP
- NORTIC A7:2025

b) Documento de **Procedimientos Operativos**, incluyendo:
- Clasificación inicial
- Revisión periódica
- Cambio de clasificación
- Gestión de excepciones
- Gestión de incidentes relacionados con mala clasificación

c) Documento formal de definición de:
- Data Owner
- Data Custodian

- Administrador Técnico
- Seguridad de la Información

d) Matriz RACI formal firmada o validada por la institución.

13.2 Componente de Concientización

a) Plan de capacitación estructurado por nivel (Alta Dirección, Mandos Medios, Colaboradores).
b) Material didáctico editable (formato abierto).
c) Evidencia de ejecución de talleres (actas o informes).

13.3 Componente Técnico

a) Documento de arquitectura técnica de la solución implementada.
b) Configuración documentada de:
- Sensitivity Labels
- Políticas de auto-etiquetado
- Políticas DLP en Microsoft 365

c) Evidencia de pruebas funcionales realizadas.
d) Informe de configuración del Microsoft Purview Information Protection Scanner, incluyendo:
- Infraestructura utilizada
- Parámetros de escaneo
- Impacto en rendimiento

e) Plan de escaneo progresivo del repositorio on-premise.
f) Reporte inicial de porcentaje de información clasificada.

13.4 Componente Integración y Control

a) Documento de integración con:
- Exchange Online
- Microsoft Defender for Endpoint
- Firewall / UTM
- Gateway de correo

b) Evidencia de configuración de controles:
- Detección
- Alertamiento
- Bloqueo automático según nivel TLP

c) Informe de pruebas de exfiltración controlada.
d) Reporte de distribución por nivel TLP.
e) Reporte de eventos DLP detectados y bloqueados.
f) Evidencia exportable para auditoría.
g) Manual operativo y playbook técnico de administración.
h) Evidencia formal de la transferencia de conocimientos.

Todos los entregables establecidos en el presente documento estarán sujetos a revisión técnica y validación formal por parte de la SIMV. En caso de que el entregable no cumpla con los requisitos técnicos, funcionales o documentales establecidos en las presentes especificaciones, la SIMV podrá rechazarlo total o parcialmente,

debiendo el proveedor realizar las correcciones correspondientes sin costo adicional, dentro del plazo que se establezca para tales fines.

14. SUBSANACIONES

A los fines del presente proceso se considera que una Oferta se ajusta sustancialmente a las Especificaciones Técnicas, cuando concuerda con todos los términos y especificaciones de dicho documento, sin desviaciones, reservas, omisiones o errores significativos. La ausencia de requisitos relativos a las credenciales de los oferentes es siempre subsanable. No se podrá considerar error u omisión subsanable, cualquier corrección que altere la sustancia de una oferta y la mejore.

Los peritos tendrán en cuenta que no deberá haber recaudos excesivos y se deberá evitar que por cuestiones formales intrascendentes se descalifiquen ofertas en perjuicio de la participación; pero salvaguardando la transparencia y la igualdad de trato para todos los oferentes.

15. CRITERIO DE EVALUACIÓN TÉCNICA Y ECONÓMICA

Las propuestas deben contener la documentación requerida en los presentes términos la cual debe ser suficiente y fehaciente para demostrar los siguientes aspectos. Por lo que, para resultar habilitado, deben cumplir con todas las especificaciones establecidas en el presente documento.

Se aplicará la modalidad de **CUMPLE/ NO CUMPLE** para la evaluación de las credenciales. **La evaluación técnica será realizada por puntaje.** La puntuación máxima asignada a la Oferta Técnica es de 85 puntos y para la Económica de 15 puntos, otorgando el mayor puntaje de evaluación económica a la oferta de menor monto y restando un punto según el orden ascendente de las demás ofertas, siendo el de mayor monto la que obtenga la puntuación más baja.

Una vez finalizada la evaluación “Sobre A”, se procederán a evaluar, exclusivamente, las respectivas Ofertas Económicas “Sobres B” de los Oferentes que hayan resultado habilitados en la evaluación de las Propuestas Técnicas, “Sobres A”.

El puntaje mínimo aceptable para la Oferta Técnica es de 80 puntos. Los proponentes que obtuviesen un puntaje inferior al señalado como mínimo, no serán habilitados para la evaluación de sus ofertas económicas “Sobres B” y serán automáticamente descalificados.

Para la evaluación de las Ofertas Técnicas se tomarán en cuenta, entre otras consideraciones, el plan de trabajo, la metodología, la experiencia, los antecedentes del equipo de trabajo, las facilidades y equipos disponibles, etc., en función de la naturaleza del proceso de contratación.

La puntuación asignada para cada uno de los renglones a evaluar es la siguiente:

Aspectos por considerar	Criterios de evaluación	Ponderación	Resultado
Propuesta técnica	Conforme al numeral **11. Servicios a requerir** del documento de Especificaciones Técnicas **(No subsanable).**	35 puntos	
Experiencia del Oferente	Presentar contrato y/o orden de compra que acredite al menos un (1) proyecto en los últimos cinco (5) años relacionados con la protección de información, en conformidad con lo establecido en **12. Otros requerimientos**, literal a) Experiencia del Oferente del documento de Especificaciones Técnicas.	20 puntos	
Perfiles y competencia del equipo técnico	Perfil del Gerente del Proyecto, certificado PMP, experiencia y habilidades para sensibilizar a los ejecutivos.	10 puntos	
	Especialista en Microsoft Information Protection, con certificaciones y experiencia demostrable.	5 puntos	
	Técnicos en Seguridad, mínimo 2 años de experiencia demostrable y competencias técnicas requeridas.	5 puntos	
Organización certificada ISO 27001 vigente	La organización certificada ISO 27001 en la gestión de sus procesos, vigente y emitida en nombre de la filial local.	5 puntos	
Acuerdo de Confidencialidad y Protección de la Información	Garantizar, mediante documento firmado y sellado, la confidencialidad y no divulgación de información sensible.	5 puntos	
	Subtotal oferta técnica	**85 puntos**	

Propuesta Económica			
Criterio económico	**Documento a evaluar**	**Ponderación**	**Resultado**
La propuesta económica detalla todos los gastos, costos y precios que correspondan, incluyendo los impuestos aplicables.	**Formulario de oferta económica (SNCC.F.033).** Presentado en **un (1) original** debidamente marcado como **"ORIGINAL"** en la primera página de la Oferta. El original deberá estar firmada en todas las páginas por el representante legal y deberán llevar el sello social de la compañía.	3 puntos	
La propuesta económica se ajusta al umbral presupuestado. **(Se restará un punto según el orden ascendente de las ofertas, siendo el de mayor monto la que obtenga la puntuación más baja)**.		8 puntos	

Propuesta Económica			
Criterio económico	**Documento a evaluar**	**Ponderación**	**Resultado**
La garantía de seriedad de la oferta se encuentra constituida correctamente en cuanto a monto y vigencia y emitida por una compañía aseguradora autorizada por la Superintendencia de Seguros para operar en la República Dominicana.	**Garantía de la Seriedad de la Oferta.** Correspondiente a un uno por ciento (1%) del monto total de la Oferta, mediante una Póliza de Fianza de una empresa de reconocida solvencia en el país.	2 puntos	
La declaración jurada o certificación de "oferta libre de colusión" se encuentra de conformidad con lo establecido en el artículo 108, numeral 3, de la Ley núm. 47-25.	**Declaración jurada o certificación de "oferta libre de colusión"**, en la que el oferente certifique que la oferta presentada es auténtica, se ha realizado de buena fe y con la intención de aceptar la adjudicación del contrato con la entidad contratante, declarando que dicha oferta se encuentra exenta de cualquier tipo de conducta o práctica colusoria, de conformidad con lo establecido en el artículo 108, numeral 3, de la Ley núm. 47-25.	2 puntos	
	Subtotal oferta económica	**15 puntos**	

El Criterio de evaluación para las Ofertas Combinadas es el siguiente:
Oferta Técnica---------- [85] puntos (OT)
Oferta Económica---------- [15] puntos (OE)

Una vez calificadas las propuestas mediante la Evaluación Técnica y Económica se procede a determinar el puntaje de estas. El puntaje total de la Propuesta será la suma de ambas evaluaciones (OT + OE). Donde:
OT = Oferta Técnica
OE = Oferta Económica

16. CRITERIO DE ADJUDICACIÓN

La adjudicación se efectuará a favor de un **único** oferente que cumpla con todos los requisitos exigidos en las especificaciones técnicas y sea calificada como la más conveniente para los intereses institucionales. Se escogerá la oferta que obtenga el mayor puntaje obtenido de la totalidad de la evaluación técnica y económica, conforme a lo establecido en el artículo 125, 126 y 127 de la Ley núm. 47-25.

17. VIGENCIA DEL CONTRATO

La vigencia del Contrato será por un período de quince (15) meses, a partir de la fecha de la suscripción del mismo y hasta su fiel cumplimiento y liquidación.

18. PLAZO PARA LA SUSCRIPCIÓN DEL CONTRATO

El Contrato deberá suscribirse en un plazo no mayor de **diez (10) días hábiles**, contados a partir de la fecha de Notificación de la Adjudicación, de conformidad con lo establecido en el artículo 134 de la Ley núm. 47-25.

19. OBLIGACIONES DEL PROVEEDOR

a) Cumplir íntegramente con el alcance, actividades, especificaciones técnicas y entregables establecidos en el presente documento.

b) Garantizar la confidencialidad, integridad y disponibilidad de la información institucional a la que tenga acceso, comprometiéndose a no divulgar, copiar ni utilizar dicha información para fines distintos a los establecidos en el contrato.

c) Implementar controles internos adecuados para la protección de la información sensible o crítica a la que acceda durante la ejecución del servicio.

d) Notificar de inmediato a la SIMV cualquier incidente de seguridad, vulnerabilidad o evento que pueda comprometer la información institucional.

e) Ejecutar el servicio conforme a buenas prácticas internacionales en materia de seguridad de la información, gobierno de datos y prevención de fuga de información.

f) Proveer el soporte post-implementación por un período no menor a seis (6) meses, conforme a lo establecido en las presentes especificaciones.

g) Entregar la documentación técnica completa, manuales y playbooks necesarios para la operación autónoma por parte del equipo interno de la SIMV.

h) No subcontratar total o parcialmente el servicio sin autorización previa y por escrito de la SIMV.

i) Asumir la responsabilidad por errores, omisiones o deficiencias derivadas de la implementación realizada.

j) Cumplir con la normativa nacional aplicable en materia de contratación pública, protección de datos y seguridad de la información.

20. PROPIEDAD INTELECTUAL

El consultor reconoce y acepta que la propiedad de toda la información desarrollada durante la consultoría será exclusiva de la Superintendencia del Mercado de Valores, por lo que el consultor se compromete a no hacer uso de esta información, en forma alguna, salvo autorización expresa y por escrito de la Superintendencia del Mercado de Valores o por algún requerimiento judicial.

21. CONTACTOS.

En caso de que exista duda o aclaración referente al proceso, suministramos los siguientes datos:

Superintendencia del Mercado de Valores de la República Dominicana.
Departamento de Compras
Teléfono: 809-221-4433, Ext. 1614
Email: comprassimv@simv.gob.do

22. FORMULARIOS TIPO.

El Oferente deberá presentar sus ofertas de conformidad con los Formularios determinados en el presente documento, los cuales se anexan como parte integral del mismo.

1. Modelo de Contrato de Servicios (SNCC.C.024)
2. Presentación Formulario de Oferta Económica (SNCC.F.033).
3. Formulario de Presentación de Oferta (SNCC.F.034)
4. Formulario de Información sobre el Oferente (SNCC.F.042).
5. Formulario de Compromiso ético de proveedores del Estado.
6. Formulario de debida diligencia.
7. Borrador de Declaración Jurada del oferente (**Recomendado**)

Elaborado y firmado digitalmente por **Rami Ramírez Saint-Hilaire**, perito técnico, **Jasmely Daniela Nin**, perito legal y **Natalio Ortiz Reyes**, perito financiero.