Santo Domingo, Distrito Nacional
26 de febrero del 2026

ESTUDIO PREVIO

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.

El artículo 87 de la Ley núm. 47-25 sobre Contrataciones Públicas establece: *"Todo procedimiento de contratación deberá estar sustentado en estudios previos, de conformidad con lo dispuesto por los reglamentos de aplicación de la presente ley y con las regulaciones especiales aplicables al objeto contractual (...)"*. En ese sentido, tenemos a bien desarrollar los siguientes puntos:

1. Necesidad de atender.

La Superintendencia del Mercado de Valores (SIMV), en su calidad de órgano regulador y supervisor del mercado de valores de la República Dominicana, administra y procesa información de carácter confidencial, sensible y estratégica, tanto de la institución como de los participantes del mercado, lo cual exige la adopción de estándares robustos de seguridad de la información.

Como parte del fortalecimiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI) y en cumplimiento del Reglamento de Ciberseguridad del Mercado de Valores, así como de los lineamientos establecidos en la NORTIC A7 y estándares internacionales como ISO/IEC 27001:2022 y NIST SP 800-53, la institución ha venido desarrollando iniciativas orientadas a robustecer su postura de seguridad, gobernanza de datos y resiliencia digital.

En este contexto, se ha identificado la necesidad de formalizar un modelo institucional de clasificación de la información que permita establecer criterios claros para la categorización, etiquetado, manejo, transmisión, retención y protección de la información institucional, bajo un esquema estructurado y alineado con buenas prácticas internacionales.

La información gestionada por la SIMV constituye un activo crítico para el cumplimiento de sus funciones regulatorias y supervisores. La ausencia de un modelo formal y homogéneo de clasificación institucional incrementa el riesgo de:

- Exposición indebida de información sensible o reservada.
- Fuga de información a través de canales electrónicos.
- Accesos no autorizados por inadecuada asignación de permisos.
- Incumplimiento de obligaciones regulatorias en materia de protección de datos.
- Impacto reputacional y pérdida de confianza en la institución.

Asimismo, en un entorno digital caracterizado por el aumento de amenazas cibernéticas, sofisticación de técnicas de exfiltración de información y mayor escrutinio regulatorio, resulta indispensable que la institución fortalezca los mecanismos preventivos y de control asociados a la protección de la información.

El proyecto implica la implementación integral de un modelo institucional que combine gobernanza, procesos, tecnología y concientización, garantizando que:

- La información sea clasificada conforme a criterios formales y documentados.
- Las etiquetas sean aplicadas de manera automática y consistente.
- Los controles DLP estén alineados al nivel de sensibilidad definido.
- Exista trazabilidad, monitoreo y evidencia para fines de auditoría.
- Los responsables de procesos asuman formalmente su rol como Data Owners.

2. Costo estimado del servicio a contratar y partida presupuestaria.

El presupuesto estimado para la "Contratación de servicios para la implementación del Sistema Institucional de Clasificación de la Información (TLP) y controles de Data Loss Prevention (DLP) para la Superintendencia del Mercado de Valores", establecido en el Plan Anual de Contrataciones (PAC), asciende a un monto de dos millones quinientos mil pesos dominicanos (RD$2,500,000.00), y que, por el tipo de servicio que vamos a adquirir, la cuenta presupuestaria para esta contratación 2.2.8.7.05, correspondiente a "Servicios de informática y sistemas computarizados".

Como parte del análisis de mercado, se revisaron propuestas técnicas y económicas recibidas de proveedores especializados en la materia. En dicho análisis se identificaron propuestas de enfoque estratégico y normativo. La empresa **Integratec** presentó una propuesta con una inversión aproximada de **USD 36,000.00**. Por su parte, la empresa **Ingenium** presentó una estimación estructurada por fases y roles especializados, con un costo total proyectado de **USD 148,266.67**.

Asimismo, se revisó el Sistema Electrónico de Contrataciones Públicas (SECP), identificándose el proceso **BAGRICOLA-CCC-LPN-2022-0006** como uno de los más recientes, adjudicado por un monto total de RD$11,461,067.33. Este proceso, diseñado para una infraestructura con mayores volúmenes de datos, presenta un alcance integral orientado a la adopción institucional y la puesta en producción de soluciones DLP, similar a lo requerido por la SIMV. El análisis comparativo evidencia que el mercado presenta una variabilidad significativa en costos y duración, dependiendo principalmente de:

- El número de procesos organizacionales impactados.
- El nivel de automatización y escaneo masivo de repositorios.
- La profundidad de integración con herramientas de seguridad existentes.
- El período de acompañamiento posterior a la implementación.
- El nivel de madurez tecnológica de la institución.

Tomando en consideración el alcance definido por la SIMV, que incluye componente de gobernanza formal, implementación técnica híbrida, integración de controles DLP y soporte posterior a la puesta en producción, se establece un presupuesto referencial ascendente a **dos millones quinientos mil pesos dominicanos (RD$2,500,000.00)**, como umbral máximo para la presente contratación.

3. Tipo de contrato a celebrarse, objeto y servicios a recibir por parte del proveedor.

Contrato de servicios. El objeto del presente proceso es la contratación de servicios especializados para el diseño, formalización e implementación del Sistema Institucional de Clasificación y Protección de la Información de la Superintendencia del Mercado de Valores (SIMV), incluyendo la configuración de mecanismos automáticos de etiquetado, la integración de controles de prevención de fuga de información (Data Loss Prevention - DLP) y el acompañamiento técnico y metodológico necesario para su puesta en producción, de conformidad con los servicios requeridos, a saber:

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.

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

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

a) Documento formal de definición de:
- Data Owner
- Data Custodian
- Administrador Técnico
- Seguridad de la Información

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

13.2 Componente de Concientización

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

13.3 Componente Técnico

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

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

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

13.4 Componente Integración y Control

h) Documento de integración con:
- Exchange Online
- Microsoft Defender for Endpoint

- Firewall / UTM
- Gateway de correo

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

h) Informe de pruebas de exfiltración controlada.
h) Reporte de distribución por nivel TLP.
h) Reporte de eventos DLP detectados y bloqueados.
h) Evidencia exportable para auditoría.
h) 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.

4. Garantías requeridas para el presente procedimiento y para la ejecución del contrato.

Los importes correspondientes a las garantías deberán hacerse en la misma moneda utilizada para la presentación de la Oferta. El Oferente/Proponente deberá presentar las siguientes garantías:

A) Garantía de la Seriedad de la Oferta

Con la finalidad de garantizar que los oferentes y eventuales adjudicatarios no retiren sin causa justificada las ofertas presentadas en el procedimiento de selección y para proteger a la Superintendencia del Mercado de Valores (SIMV), ante dicho incumplimiento, los oferentes/proponentes deberán constituir una garantía de seriedad de su oferta, que esté vigente por un período no menor a **treinta (30) días hábiles** contados a partir de la fecha del acto de apertura de la oferta técnica, y que cumpla con las siguientes características:

1- Póliza por un monto equivalente a **uno por ciento (1%)** del monto de la oferta a presentar.
2- En la misma moneda de la oferta, dígase en pesos dominicanos, RD$.
3- En beneficio de la Superintendencia del Mercado de Valores (SIMV).
4- Incondicional, irrevocable y renovable.
5- Garantía de Seriedad de la oferta en origina: Correspondiente a una póliza, por un valor del uno por ciento (1%) del monto total de la Oferta. La vigencia no deberá ser menor a **treinta (30) días hábiles**, contados a partir de la fecha del acto de apertura de Ofertas Técnicas.

Párrafo I. La Garantía de Seriedad de la Oferta será de cumplimiento obligatorio, mediante una Póliza de Fianzas, emitida por una compañía aseguradora en la República Dominicana y vendrá incluida dentro de la Oferta Económica "Sobre B", de conformidad con lo establecido en el artículo 202 del Decreto 52-26 del Reglamento de Aplicación de la Ley núm. 47-25, sobre Contrataciones Públicas.

B) Garantía de Fiel Cumplimiento de Contrato

Para poder suscribir el contrato el adjudicatario deberá constituir previamente una garantía de fiel cumplimiento de contrato a favor de la Superintendencia del Mercado de Valores (SIMV), para asegurar que cumplirá con las obligaciones y clausulas establecidas en el presente documento y en el contrato y que los servicios sean entregados de acuerdo con las condiciones y requisitos previsto en el presente documento, la oferta adjudicada y el propio contrato. La garantía deberá ser emitida por una compañía aseguradora autorizada por la Superintendencia de Seguros para operar en la República Dominicana.

El Adjudicatario cuyo contrato exceda el equivalente en Pesos Dominicanos de diez mil dólares de los Estados Unidos de Norteamérica con cero centavos (US$10,000.00), está obligado a constituir una Póliza de Fianzas emitida por una compañía aseguradora en la República Dominicana, en el plazo de **cinco (5) días hábiles**, contados a partir de la Notificación de la Adjudicación, por el importe del CUATRO POR CIENTO (4%) del monto total del Contrato a intervenir, a disposición de la Entidad Contratante, cualquiera que haya sido el procedimiento y la forma de Adjudicación del Contrato. Para el caso de las micro, pequeñas y medianas empresas (MIPYMES), el monto de la garantía de fiel cumplimiento será equivalente al UNO POR CIENTO (1%) del monto de la adjudicación.

Si posterior a la firma del contrato se genera una modificación al monto del mismo, deberá renovar la garantía de fiel cumplimiento en donde se garantice el nuevo monto establecido.

La vigencia de la garantía será de mínimo 15 meses, contados a partir de la constitución de la misma y hasta el fiel cumplimiento, incluyendo un plazo adicional de 1 mes con posterioridad a la fecha de liquidación del contrato.

La no comparecencia del Oferente Adjudicatario a constituir la Garantía de Fiel Cumplimiento de Contrato se entenderá que renuncia a la Adjudicación y se procederá a la ejecución de la Garantía de Seriedad de la Oferta.

Cuando hubiese negativa a constituir la Garantía de Fiel Cumplimiento de Contrato, la Entidad Contratante, como Órgano de Ejecución del Contrato, notificará la Adjudicación de los renglones correspondientes al Oferente que hubiera obtenido la siguiente posición en el proceso de Adjudicación, conforme al Reporte de Lugares Ocupados. El nuevo Oferente Adjudicatario depositará la Garantía y suscribirá el Contrato de acuerdo al plazo que le será otorgado por la Entidad Contratante, mediante comunicación formal.

C) Garantía de buen uso de anticipo

El (los) oferente (s) estarán obligados a constituir la Garantía de Buen Uso del Anticipo, equivalente al cien por ciento (100%) de los montos que reciba por concepto del Primer Pago o Anticipo, mediante una Póliza de Fianza emitida por una compañía aseguradora en la República Dominicana, se hará en un plazo no mayor treinta (30) días a partir de la certificación del Contrato y contra presentación de una garantía de buen uso de anticipo de tipo Póliza de Seguro que cubra la totalidad del Avance Inicial.

La garantía de buen uso de anticipo será devuelta cuando el (la) contratista demuestre que cumplió con todas las obligaciones del contrato. El monto máximo que será devuelto debe ser igual al monto dado como anticipo.

5. Requisitos de calificación para asegurar las condiciones profesionales, técnicas y financieras para satisfacer el objeto contractual.

A. PROFESIONALES

1) Formulario de Información sobre el Oferente (**SNCC.F.042**).
2) Formulario de Compromiso ético de Proveedores (as) del Estado de la Dirección General de Contrataciones Públicas;
3) Copia del Registro Nacional de Proveedores (RPE), emitido por la Dirección General de Contrataciones Públicas (Activo);
4) Certificado de Registro Mercantil, VIGENTE;
5) Copia legible y vigente del documento de identidad del representante legal;
6) Copia de los Estatutos Sociales del Oferente, debidamente registrados en el Registro Mercantil correspondiente.
7) Copia de la última Acta de Asamblea que contenga la designación del representante legal.
8) Copia de la Nómina de Accionistas con composición accionaria actualizada, debidamente registrada en el Registro Mercantil correspondiente.
9) Poder de representación (Si aplica).
10) Certificación Micro, Pequeñas y Medianas Empresas (MIPYMES) (cuando aplique).
11) Original de Declaración Jurada del oferente, firmada por su representante legal y sellada con el sello de la sociedad. Esta Declaración Jurada debe ser notarizada (firmada y sellada), por un Notario Público. **(se recomienda utilizar el borrador adjunto en el SECP en la carpeta de "Formularios").** Esta Declaración debe ser redactada con las adaptaciones o ajustes correspondientes al nombre del oferente y en primera persona, no transcrita literalmente y debe contener lo siguiente:
    a. Que no se encuentra dentro de las inhabilidades para contratar establecidas en el artículo 38 de la Ley núm. 47-25 y donde manifieste si tiene o no litigio en curso con el Estado Dominicano o sus entidades del Gobierno Central, de las Instituciones Descentralizadas y Autónomas no financieras, o con Instituciones Públicas de la Seguridad Social;

b. Que en la cual expresamente declare que la Empresa no está sujeta a procedimiento de quiebra o bancarrota, liquidación, concurso de acreedores, ni que sus actividades han sido suspendidas y que no es deudora de entidad estatal y/o privada que pueda comprometer la ejecución de cualquier Contrato, de acuerdo a lo establecido en el Artículo 37 de la mencionada Ley núm. 47-25;
c. Que ni el Proponente ni su personal directivo ha sido condenados por un delito relativo a su conducta profesional o por declaración falsa o fraudulenta acerca de su idoneidad para firmar un contrato adjudicado;
d. Si sus socios o accionistas, junta de directores o representantes legales son o han sido persona(s) expuesta(s) políticamente (PEP) conforme a lo definido en la Ley contra el Lavado de Activos. (Si es positivo, establecer cargo (s), fecha(s) de designación, remoción y país);
e. Licitud de su patrimonio;
f. Identifique el/los beneficiarios (s) final (es) conforme a las disposiciones de la Ley núm. 155-17, firmada por el representante legal de su empresa.

B. FINANCIEROS

1. Certificación emitida por la Dirección General de Impuestos Internos (DGII), donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones fiscales;
2. Certificación emitida por la Tesorería de la Seguridad Social, donde se manifieste que el oferente se encuentra al día en el pago de sus obligaciones de la Seguridad Social (TSS), solo aplicará cuando se trate de una persona jurídica, conforme a lo establecido en la Ley núm. 87-01, que crea el Sistema Dominicano de Seguridad Social;

C. TÉCNICOS

1) Formulario de Presentación de Oferta (SNCC.F.034).
2) Propuesta técnica (conforme al numeral **11. Servicios a requerir** del documento de Especificaciones Técnicas **(No subsanable).**
3) Presentación de los documentos que demuestren evidencias de los requisitos solicitados en el numeral **12. Otros requerimientos,** del documento de Especificaciones Técnicas.

Firmado digitalmente por el señor **Roberto Quezada Domínguez**, Director de Tecnología de la Información y Comunicaciones, **Sarah E. Roa Ramírez**, Directora Jurídica y **Mariella E. Troncoso Freites**, en representación de la señora **Milli M. Núñez Cruz**, Directora Administrativa y Financiera.