

INFORME JUSTIFICATIVO

Renovación de la Suscripción de la Plataforma de Gestión de Exposición y Vulnerabilidades Rapid7 por un período de tres (3) años

Dirigido a: Comité de Compras y Contrataciones

Por medio del presente informe se remite al Comité de Compras la justificación técnica, operativa y económica que sustenta la necesidad de **renovar y ampliar la suscripción de la plataforma Rapid7**, migrando del licenciamiento actual de **InsightVM (Plataforma básica)** hacia **Exposure Command (Plataforma avanzada)**, con una cobertura de **2,000 activos** y una vigencia de **tres (3) años**. La plataforma se encuentra en operación ininterrumpida en la institución desde el año **2021** y su suscripción se encuentra actualmente **vencida y en período de gracia otorgado por el fabricante**, por lo que la decisión sobre su renovación reviste de carácter de urgencia a fin de evitar la suspensión de un control de seguridad actualmente operativo.

DIAGNÓSTICO GENERAL

Antecedentes de la contratación

La plataforma Rapid7 se encuentra desplegada y en operación en la institución desde el año **2021** en **DGA**. Durante el período comprendido entre **2021 y 2024** su licenciamiento fue renovado mediante contrataciones de **vigencia anual**, esquema que obligó a ejecutar un proceso de compra por cada ejercicio presupuestario. En el año **2024** se adoptó por primera vez un esquema plurianual, contratándose **Rapid7 InsightVM** por un período de **dos (2) años**, con una cobertura de **ochocientos (800) activos** y por un monto de **RD\$7,080,000.00**.

Período	Modalidad de contratación	Observación
2021 - 2024	Renovaciones de vigencia anual.	Un proceso de compra por año; exposición recurrente a ajustes de precio y a riesgo de interrupción.
2024 - 2026	Contratación bianual — InsightVM, 800 activos, RD\$7,080,000.00.	Primer esquema plurianual; mejora en condiciones respecto al ciclo anual.
Situación actual	Suscripción vencida, operando bajo período de gracia del fabricante.	El servicio continúa temporalmente activo, pero sin cobertura contractual vigente.

Situación de vigencia: período de gracia

Al momento de la elaboración del presente informe, la suscripción **ya ha superado su fecha de vencimiento contractual** y la continuidad del servicio se sostiene exclusivamente en el **período de gracia otorgado por el fabricante**, concedido con el propósito de permitir la formalización de la renovación. Dicho período es de duración limitada y de carácter discrecional, por lo que no constituye una condición sobre la cual la institución pueda planificar su operación.

Esta circunstancia implica que la institución opera actualmente un control de seguridad crítico sin respaldo contractual vigente. De agotarse el período de gracia sin que se haya formalizado la renovación, la suspensión del servicio sería inmediata y automática, sin que exista mecanismo de continuidad alternativo. En consecuencia, el presente proceso no admite dilación.

Evolución de las condiciones de operación

A lo largo de sus cinco (5) años de operación, la plataforma se ha consolidado como la herramienta institucional de referencia para la evaluación continua de vulnerabilidades, la generación de reportes de cumplimiento y el soporte a los procesos de auditoría en materia de seguridad de la información. No obstante, dos factores han modificado sustancialmente las condiciones bajo las cuales se dimensionó originalmente el servicio:

- **El incremento del inventario de activos**, por el crecimiento del parque tecnológico institucional, la incorporación de nuevos servicios digitales, la expansión de la infraestructura virtualizada y en nube, y la adición de equipos y dispositivos que hoy quedan fuera del alcance de la licencia.
- **La evolución del perfil de riesgo institucional**, cuya superficie de ataque ya no se limita a los activos internos escaneables, sino que incluye activos expuestos a Internet, cargas de trabajo en nube, identidades y aplicaciones, componentes que el licenciamiento actual no contempla.

En consecuencia, la cobertura contratada de 800 activos resulta insuficiente frente al inventario real, generando una brecha de visibilidad que constituye hoy el principal riesgo de ciberseguridad no mitigado de la institución.

PROBLEMÁTICA IDENTIFICADA

Cobertura de licenciamiento insuficiente

El esquema vigente permite el escaneo y monitoreo de un máximo de 800 activos. Todo activo que exceda dicho límite permanece fuera del alcance de la plataforma, lo que implica que:

- **No se evalúan sus vulnerabilidades** sin que existan controles compensatorios equivalentes.
- **No aparecen en los tableros de riesgo institucional** ni en los reportes de cumplimiento.
- **Se genera una métrica de riesgo distorsionada**, por cuanto los indicadores se calculan sobre un universo parcial.
- **Se mantiene un punto ciego explotable**, dado que un solo activo no monitoreado puede constituir el punto de entrada a la red institucional.

Visibilidad fragmentada de la superficie de ataque

La gestión tradicional de vulnerabilidades responde a la pregunta de qué debilidades existen en los activos escaneados, pero no correlaciona dichas debilidades con la exposición real hacia Internet, las configuraciones erróneas en nube, las identidades privilegiadas ni los riesgos a nivel de aplicación. Esta fragmentación produce:

- **Priorización basada únicamente en severidad técnica (CVSS), sin contexto de explotabilidad ni de criticidad para el negocio.** De forma manual y con criterios heterogéneos entre equipos.
- **Esfuerzo analítico duplicado.** Ya que el personal técnico debe consolidar información proveniente de fuentes distintas para determinar qué remediar primero.
- **Tiempos de remediación extendidos.** Entre el momento en que se identifica una vulnerabilidad crítica y el momento en que efectivamente se corrige.

Riesgo de discontinuidad del servicio

Agotado el período de gracia sin que se haya formalizado la renovación, se produciría la pérdida inmediata de las capacidades de escaneo autenticado, monitoreo continuo, actualización de la base de conocimiento de vulnerabilidades y acceso a la inteligencia de amenazas del fabricante. La institución quedaría, en la práctica, sin capacidad de evaluación de vulnerabilidades, con las siguientes consecuencias:

- Interrupción de la evidencia de cumplimiento requerida por los órganos de control y por los procesos de auditoría interna y externa.
- Pérdida del histórico operativo y de las líneas base de configuración construidas de forma acumulativa desde el año 2021.
- Exposición no gestionada frente a vulnerabilidades de divulgación reciente y de explotación activa.
- Costos de reactivación, redespiegue y reconstrucción de la configuración, sustancialmente superiores a los de mantener la continuidad del servicio.

IMPACTO INSTITUCIONAL

Tipo de Impacto	Descripción
Operativo	Activos fuera de cobertura que no son evaluados; priorización manual de vulnerabilidades y consolidación de información desde fuentes dispersas.
Económico	Costo de una eventual materialización de incidentes; sobre costo de reactivar el servicio tras una interrupción; pérdida del valor de la inversión ya realizada.
Regulatorio	Dificultad para evidenciar el cumplimiento de la NORTIC A7, la Ley 172-13 sobre Protección de Datos Personales y las disposiciones del Decreto 539-20 en materia de ciberseguridad.
Estratégico	Indicadores de riesgo calculados sobre un universo parcial de activos, lo que compromete la calidad de la toma de decisiones en materia de seguridad.
Imagen institucional	Exposición reputacional ante un incidente de seguridad originado en un activo no monitoreado.
Riesgo legal	Responsabilidad institucional derivada de la afectación de datos personales o de la interrupción de servicios por vulnerabilidades conocidas y no remediadas.

SITUACIÓN ACTUAL DEL LICENCIAMIENTO

La suscripción vigente presenta las siguientes características y limitaciones:

Componente	Alcance actual	Limitación
Plataforma	Rapid7 InsightVM sobre Insight Platform.	Cubre gestión de vulnerabilidades, sin gestión de superficie de ataque ni contexto de nube.
Cobertura	800 activos licenciados.	Insuficiente frente al inventario real; los activos excedentes quedan sin evaluación.
Vigencia	Bianual (2024-2026); precedida de renovaciones anuales desde 2021.	Suscripción vencida y en período de gracia; los ciclos cortos han obligado a renegociar de forma recurrente y con menor poder de negociación.
Priorización	Basada en severidad técnica y en el contexto del activo escaneado.	No incorpora exposición externa, identidades ni configuraciones de nube en el modelo de riesgo.
Remediación	Proyectos de remediación dentro de la propia consola.	Sin orquestación centralizada ni automatización nativa hacia las herramientas de gestión de servicios.

SOLUCIÓN PROPUESTA Y BENEFICIOS ESPERADOS

Se propone la renovación de la suscripción bajo la modalidad **Rapid7 Exposure Command**, ampliando la cobertura a **2,000 activos** por un período de **tres (3) años**. Exposure Command incorpora el mismo motor de escaneo de InsightVM y lo integra con capacidades de gestión de superficie de ataque, seguridad en nube y contexto de identidades sobre la Command Platform del fabricante, consolidando en un único modelo de riesgo la información que hoy se analiza de forma fragmentada.

Beneficio	Descripción
Cobertura completa del inventario	Ampliación de 800 a 2,000 activos, eliminando los puntos ciegos actuales y permitiendo que las métricas de riesgo reflejen la totalidad del parque tecnológico.
Visión unificada del riesgo	Correlación de vulnerabilidades, activos expuestos a Internet, cargas de trabajo en nube e identidades dentro de un mismo modelo de priorización.
Priorización por riesgo real	Ordenamiento de las exposiciones según explotabilidad activa e inteligencia de amenazas del fabricante, y no únicamente por severidad teórica.
Remediación orquestada	Asignación, seguimiento y validación centralizada de las correcciones, con automatización hacia las herramientas de gestión de servicios ya utilizadas por la institución.
Continuidad operativa	Preservación del histórico, de las líneas base y de la configuración desplegada, sin costos ni tiempos de redespigue.
Cumplimiento y auditoría	Evidencia sistemática y trazable para los procesos de auditoría y para la demostración de cumplimiento ante los órganos de control.

Beneficio	Descripción
Aprovechamiento de la curva de aprendizaje	El personal técnico ya se encuentra capacitado en la plataforma, lo que elimina los costos de adopción asociados a un cambio de fabricante.

ANÁLISIS ECONÓMICO DE LA PROPUESTA

A fin de dimensionar correctamente la inversión solicitada, se presenta a continuación la comparación entre el contrato vigente y la propuesta de renovación:

Concepto	Contrato 2024 (InsightVM)	Propuesta (Exposure Command)
Activos licenciados	800	2,000
Vigencia	2 años	3 años
Monto total	RD\$7,080,000.00	RD\$19,500,000.00
Costo anual	RD\$3,540,000.00	RD\$6,500,000.00
Costo por activo / año	RD\$4,425.00	RD\$3,250.00

El elemento central de este análisis es el **costo unitario por activo**. Si bien el monto total de la contratación se incrementa, ello obedece a que la cobertura crece un 150% y el plazo se extiende de dos a tres años. Medida sobre una base homogénea, la propuesta representa una **reducción del 26.6% en el costo por activo por año**, pasando de RD\$4,425.00 a RD\$3,250.00.

Dicho de otro modo: renovar el licenciamiento actual de InsightVM para 2,000 activos durante tres años, manteniendo el precio unitario vigente, representaría una erogación aproximada de RD\$26,550,000.00. La propuesta de Exposure Command asciende a RD\$19,500,000.00, lo que implica:

- **Un ahorro estimado de RD\$7,050,000.00** respecto al escenario de extender el licenciamiento actual a la misma cobertura y plazo.
- **La incorporación de capacidades superiores de gestión de superficie de ataque y de exposición**, sin costo incremental por dicha ampliación de alcance.

JUSTIFICACIÓN DEL PLAZO DE TRES (3) AÑOS

La contratación por un período de tres años responde a criterios técnicos y económicos concretos:

1. **Corrección de un patrón de contratación ineficiente.** Entre 2021 y 2024 la plataforma fue renovada bajo vigencia anual, lo que obligó a ejecutar un proceso de compra por ejercicio y expuso a la institución de forma recurrente al riesgo de interrupción del servicio. La contratación bianual de 2024 constituyó una primera corrección; el plazo de tres años consolida esa mejora.

2. **Mejores condiciones económicas.** El compromiso plurianual es el mecanismo que permite obtener la reducción del costo unitario descrita en el apartado anterior; una contratación anual o bianual no accede a dicha estructura de precios.
3. **Protección frente a la variación de precios.** Se fija el costo del servicio por tres ejercicios presupuestarios, eliminando la incertidumbre asociada a incrementos de tarifa y a la variación cambiaria.
4. **Reducción de la carga administrativa.** Se evita la ejecución de dos procesos de contratación adicionales durante el mismo horizonte temporal, con el consiguiente ahorro de tiempo y de recursos institucionales.
5. **Continuidad del programa de seguridad.** La gestión de vulnerabilidades es un proceso continuo y de maduración progresiva; los ciclos cortos de contratación introducen riesgo de interrupción y afectan la consistencia de las métricas históricas.
6. **Horizonte de implementación.** La incorporación de las capacidades de gestión de superficie de ataque y de nube requiere un período de despliegue, ajuste y maduración que excede un ciclo anual.

RECOMENDACIÓN

Con base en el diagnóstico presentado y en el análisis económico expuesto, se recomienda al Comité de Compras:

1. **Declarar la urgencia del proceso**, en atención a que la suscripción se encuentra vencida y operando bajo período de gracia del fabricante, condición temporal y discrecional cuyo agotamiento produciría la suspensión inmediata del servicio.
2. **Aprobar la renovación y ampliación** de la suscripción de la plataforma Rapid7 bajo la modalidad Exposure Command, para 2,000 activos y por un período de tres (3) años, conforme a los Términos de Referencia que se acompañan como anexo a este informe.
3. **Autorizar el inicio del proceso de contratación** correspondiente, de conformidad con lo establecido en la Ley N° 47-25 sobre Compras y Contrataciones Públicas y su Reglamento de Aplicación, considerando la naturaleza propietaria de la solución y las condiciones de exclusividad aplicables a la renovación de licenciamiento del fabricante.
4. **Considerar este proceso como prioritario** para la institución, en virtud de que:
 - La suscripción se encuentra vencida y la continuidad del servicio depende de un período de gracia de duración limitada.
 - Se trata de la continuidad de un control de seguridad en operación ininterrumpida desde el año 2021, y no de una adquisición nueva.
 - Permite eliminar la brecha de visibilidad existente sobre los activos no licenciados.
 - Representa una reducción real del costo unitario del servicio respecto al contrato vigente.
 - Consolida en una sola plataforma capacidades que de otro modo requerirían contrataciones adicionales.

Como parte de la documentación de respaldo del presente proceso, se incorpora la carta emitida por Peter Kaes, vicepresidente de Asuntos Legales Comerciales de Rapid7, mediante la cual el fabricante certifica que las empresas:

- Sidif del Caribe
- Adexsus
- CSTISA

Son los únicos socios autorizados para presentar propuestas, comercializar, distribuir y brindar soporte técnico de las soluciones Rapid7 en el proceso de contratación convocado por la Dirección General de Aduanas para el período 2026. Asimismo, el fabricante confirma que dichos socios cuentan con el nivel de certificación, la capacidad técnica y el respaldo comercial directo requeridos para participar en el presente proceso, lo que sustenta las condiciones de exclusividad asociadas a la renovación y ampliación del licenciamiento objeto de esta contratación.

CONCLUSIONES

Se concluye que:

Conforme a lo indicado en el informe de justificación, la plataforma **Rapid7** forma parte de las herramientas especializadas utilizadas por la institución para la gestión proactiva de vulnerabilidades, identificación de riesgos de seguridad y fortalecimiento continuo de la postura de ciberseguridad institucional.

La renovación de estas licencias es necesaria para garantizar la continuidad de las capacidades de monitoreo, detección y análisis de vulnerabilidades de los activos tecnológicos de la institución. La interrupción del servicio podría afectar la visibilidad sobre riesgos de seguridad existentes y emergentes, así como limitar las capacidades para identificar, priorizar y remediar vulnerabilidades de manera oportuna, incrementando la exposición a amenazas cibernéticas.

Asimismo, la herramienta permite disponer de un inventario centralizado de activos, evaluación continua de vulnerabilidades, generación de informes especializados, análisis de exposición y seguimiento de las acciones de mitigación, funciones que resultan esenciales para las operaciones de la Gerencia de Ciberseguridad y para el cumplimiento de las buenas prácticas de seguridad de la información.

De acuerdo con el estudio de mercado realizado y la comunicación emitida por el fabricante **Rapid7**, en la República Dominicana únicamente existen tres (3) empresas autorizadas como socios comerciales para la comercialización y prestación de servicios asociados a esta solución, por esta razón, procede la utilización del procedimiento de excepción por exclusividad, conforme a las disposiciones establecidas en la normativa de compras y contrataciones públicas aplicable. Anexamos carta del fabricante.

1. **La cobertura actual de 800 activos es insuficiente** frente al inventario tecnológico real de la institución, generando puntos ciegos de seguridad que no cuentan con controles compensatorios equivalentes.
2. **La suscripción se encuentra vencida y en período de gracia**, condición temporal y de carácter discrecional del fabricante. Su agotamiento sin renovación formalizada dejaría a la institución sin

capacidad de evaluación continua de vulnerabilidades, con impacto directo sobre la operación, el cumplimiento normativo y el riesgo institucional.

3. **La migración a Exposure Command** no constituye una adquisición nueva, sino la evolución natural de una plataforma en operación ininterrumpida desde el año 2021, ya desplegada, operada y conocida por el personal técnico, lo que elimina los costos y riesgos asociados a un cambio de fabricante.
1. **La propuesta es económicamente ventajosa**, por cuanto reduce en un 26.6% el costo por activo por año y representa un ahorro estimado de RD\$7,050,000.00 frente al escenario de extender el licenciamiento vigente a la misma cobertura y plazo.
2. **El plazo de tres (3) años** corrige el patrón de renovaciones de ciclo corto sostenido entre 2021 y 2024, es el que permite acceder a las condiciones económicas señaladas y el que resulta consistente con el horizonte de maduración del programa institucional de gestión de vulnerabilidades.

FINANCIAMIENTO

La renovación solicitada asciende a un monto total de **RD\$19,500,000.00** por los tres (3) años de vigencia, equivalente a **RD\$6,500,000.00 anuales**. Se tiene previsto que la contratación sea ejecutada con cargo a las partidas contempladas en el **Plan Anual de Compras y Contrataciones (PACC)**, sin afectar la continuidad de las operaciones institucionales ni otros compromisos presupuestarios previamente asumidos.

La inversión en esta solución se **justifica plenamente** por la continuidad del control de seguridad, la eliminación de la brecha de cobertura, la reducción del costo unitario del servicio y la mitigación de riesgos legales, regulatorios y reputacionales asociados a la gestión de vulnerabilidades. Por todo lo expuesto, se **solicita la aprobación del proceso de compra** conforme a los Términos de Referencia presentados.

Carlos David Acosta Siri
Encargado de Departamento Operaciones Cibernéticas.