ANÁLISIS DEL SECTOR

De conformidad con lo normado en el numeral 12 del artículo 25 de la ey 80 de 1993, en el numeral 2 del artículo 5 de la Ley 1150 de 2007 y en el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015 y de acuerdo con el Plan anual de adquisiciones del INPEC bajo la posición del catálogo de gasto C-1299-0800-7-40020112-1299085-02 MODERNIZACION INTEGRAL DE LAS CAPACIDADES TECNOLOGICAS DEL INPEC A NIVEL NACIONAL, en coordinación con la Oficina de Sistemas de Información, se procede a realizar el siguiente Análisis del Sector para la adquisición de una **"SOLUCIÓN DE COMUNICACIÓN DE RED"**.

1. ASPECTOS GENERALES

La incorporación de una plataforma especializada para el monitoreo proactivo de la red y la experiencia digital (NPM – *Network Performance Monitoring* / DEM – *Digital Experience Monitoring*) reviste una importancia estratégica y operativa fundamental para el Instituto Nacional Penitenciario y Carcelario – INPEC.

En primer lugar, la continuidad operativa de la entidad depende de manera crítica de la disponibilidad permanente de sus sistemas tecnológicos. Plataformas como el registro biométrico de internos, la videovigilancia en tiempo real, el correo electrónico, SISIPEC, GESDOC y el Software Humano, constituyen el corazón de la operac ón penitenciaria y administrativa. Una falla en las comunicaciones o la degradación en el rendimiento de la red puede colapsar estos servicios, afectando los procesos esenciales en los establecimientos de reclusión a nivel nacional.

Actualmente, carecer de una visibilidad profunda (capa 2 a capa 7) genera tiempos de respuesta prolongados ante incidentes (alto MTTR - *Mean Time to Resolution*). La adopción de una solución de monitoreo unificada actúa como un mecanismo de optimización que minimiza la probabilidad de caídas del servicio, permitiendo detectar cuellos de botella antes de que afecten al usuario final.

Además, en el entorno actual de TI, el monitoreo y la ciberseguridad deben converger. Es un imperativo técnico que esta nueva herramienta se integre de manera nativa (vía API) con el ecosistema de seguridad perimetral e interno (Security Fabric) ya existente en el INPEC. Esta integración permite correlacionar eventos de red con eventos de seguridad en tiempo real y ejecutar remediaciones automáticas, fortaleciendo la resiliencia tecnológica de la Institución.

ECONÓMICO

El Instituto Nacional Penitenciario y Carcelario – INPEC administra un presupuesto anual de $2,2 billones de pesos para 2026, según la Resolución 00001 del 2 de enero de 2026, que aprobó la distribución de los recursos del Presupuesto General de la Nación[1]. En este marco, el proceso de contratación reserva $400.000.000 pesos M/Cte para la adquisición de la Solución de Comunicación de Red. A la TRM del 18 de febrero de 2026 ($3.664,26

[1] https://inpec.gov.co/documents/d/guest/r000001_02012026?download=true#:~:text=apropi%C3%B3%20al%20Instituto%20Nacional%20Penitenciario,601.045.486)%20MONEDA%20CORRIENTE.

COP/USD), dicho rubro equivale aproximadamente a USD $ 109.162. Desde la perspectiva de las finanzas públicas, este monto representa apenas el 0,018% del presupuesto institucional, pero protege procesos cuya indisponibilidad, degradación o vulneración puede generar pérdidas muy superiores a ese porcentaje.

La magnitud del riesgo de no contar con una visibilidad profunda y proactiva de la red se ilustra con la estadística de Cybersecurity Ventures[2], que calcula que los daños globales por incidentes cibernéticos (los cuales suelen propagarse lateralmente por las redes sin ser detectados a tiempo) alcanzarán los USD $275.000 millones anuales en 2031. En paralelo, IBM Security[3] reporta que el costo promedio de una interrupción grave de sistemas fue de USD $4,45 millones, destacando que la falta de herramientas de monitoreo integradas a la seguridad aumenta drásticamente el tiempo para identificar y contener los incidentes. Si el INPEC llegara a enfrentar una indisponibilidad prolongada de sus sistemas críticos por fallas de comunicación no detectadas, el impacto financiero podría superar varias veces el valor de la inversión proyectada.

Aun en escenarios conservadores —como una falla de enrutamiento o un cuello de botella que derive en la incisponibilidad de sistemas misionales (como SISIPEC o GESDOC) por 24 horas— los costos en pérdida de productividad, horas extras de soporte y afectación operativa se ubicarían muy por encima de los USD $200.000, es decir, más de dos veces el valor del proyecto. El factor diferencial está en la rapidez y efectividad de la detección; las soluciones de monitoreo de red de última generación aseguran una identificación proactiva de las anomalías de tráfico en tiempo real, reduciendo drásticamente el Tiempo Medio de Resolución (MTTR) y la probabilidad de que se materialicen interrupciones de alto impacto.

En conclusión, la inversión prevista neutraliza pérdidas probables de alto costo, blinda las operaciones esenciales de los establecimientos de reclusión y posiciona al INPEC por delante de una curva de riesgo tecnológico que crece de manera exponencial. Así, el rubro destinado deja de ser un gasto y se convierte en un seguro de continuidad, eficiencia operativa y responsabilidad fiscal frente a los recursos de los colombianos.

REGULATORIO

La contratación de una Solución de Comunicación de Red en el Instituto Nacional Penitenciario y Carcelario – INPEC se sustenta, en primer término, en el marco jurídico superior de la contratación estatal colombiana. Con arreglo a la Constitución Política, dicho marco lo integran la Ley 80 de 1993 (Estatuto General de la Contratación Pública), la Ley 1150 de 2007 (por la cual se introducen medidas para la eficiencia y transparencia), la Ley 1474 de 2011 (Estatuto Anticorrupción), las normas orgánicas del presupuesto, el Estatuto Tributario, las disposiciones cambiarias y toda otra norma que regule la materia durante la vigencia del proceso.

En particular, el numeral 12 del artículo 25 de la Ley 80 exige la elaboración de estudios previos que acrediten necesidad, conveniencia e idoneidad, así como suficiencia de recursos; al tiempo, impone los principios de planeación, transparencia y economicidad

[2] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/?utm

[3] https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs?utm

que rigen el gasto público. Conexamente, el Decreto 1082 de 2015 reglamenta las disposiciones de la Ley 80 y, en su artículo 2.2.1.1.2.1.1, fija el contenido mínimo de los estudios previos: análisis de mercado, riesgos, especificaciones técnicas, modalidad de selección y fuentes de financiación. Tal artículo actúa como manual procedimental que estandariza los formatos y etapas del ciclo contractual, garantizando trazabilidad y control.

En el plano institucional específico, el Decreto 4151 de 2011 atribuye a la Oficina de Sistemas de Información la formulación y ejecución de la política TIC del INPEC; su artículo 12 le encomienda planear y supervisar la adquisición de soluciones tecnológicas clave para la continuidad del servicio penitenciario. Esa competencia se reafirma en la Resolución Interna 0243 de 2020, cuyo artículo 19 formalizó el Grupo de Administración de Tecnologías de la Información como dependencia responsable de diagnosticar necesidades, proyectar compras y administrar la infraestructura tecnológica, de redes y de comunicaciones de la Entidad.

La Política de Gobierno Digital constituye el marco estratégico en materia de servicios al ciudadano. Sus directivas obligan a que la información pública se ofrezca de forma óptima, segura y ágil, premisa que exige sistemas de comunicación permanentemente actualizados, monitoreados y alineados con los estándares del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Precisamente, la Resolución 500 de 2021 del MinTIC adopta el Modelo de Seguridad y Privacidad de la Información MSPI como habilitador de dicha política y obliga a todas las entidades estatales a desplegar controles que aseguren la confidencialidad, integridad y disponibilidad de la información: la implementación de herramientas para el monitoreo y visibilidad de la red se reconoce expresamente como una salvaguarda esencial para garantizar la disponibilidad de los servicios críticos.

A nivel sectorial, diversos estudios empresariales advierten que la carga tributaria y la dispersión de obligaciones regulatorias se perciben como barreras a la inversión tecnológica; sin embargo, los mismos informes coinciden en que la adopción de tecnologías de punta para la observabilidad y el monitoreo incrementa la productividad, optimiza costos y mejora la prestación del servicio público. En el entorno penitenciario, las fallas de comunicación y los eventos de interrupción de red ocurridos en los últimos años han evidenciado la necesidad de reforzar los mecanismos de diagnóstico, detección de anomalías de tráfico y optimización de rutas para salvaguardar la operación misional.

Así, la decisión de invertir en una Solución de Comunicación de Red no responde únicamente a la conveniencia técnica, sino al cumplimiento expreso de mandatos legales y programáticos: (i) dar aplicación a los principios de la contratación estatal, (ii) atender la Política de Gobierno Digital y el MSPI, (iii) materializar las competencias que el Decreto 4151 y la Resolución 0243 asignan a la Oficina de Sistemas y al Grupo de Administración de TI, y (iv) proteger y garantizar la disponibilidad de la infraestructura tecnológica penitenciaria frente a interrupciones o riesgos digitales que comprometerían la seguridad nacional y los derechos fundamentales. Este entramado normativo, conocido y obligatorio para todos los proponentes, confiere legitimidad y coherencia institucional al proceso de selección y al contrato resultante.

1. ANÁLISIS DE LA DEMANDA

1.1. Histórico de la Entidad

La entidad no ha realizado contrataciones con objeto igual o similar al requerido.

1.2. Análisis Intersectorial

Para efectuar el estudio de mercado, se realizó la consulta en la plataforma SECOP II, verificando los procesos contractuales registrados por diferentes entidades estatales, cuyos fines y actividades guardan correspondencia o afinidad con lo requerido en el presente Estudic, lcs cuales se detallan en la siguiente tabla:

AÑO	ENTIDAD	No. CONTRATO	OBJETO	VALOR TOTAL DEL CONTRATO	ESTADO DEL PROCESO
2025	AEROCIVIL	25001412 H3	Realizar el mejoramiento del sistema de monitoreo y seguridad CCTV del aeropuerto internacional Ernesto Cortissoz	$ 1.400.000.000	Proceso adjudicado y celebrado
2024	INSTITUTO DE DESARROLLO URBANO	IDU-SAMC-DTAF-001-2024	Prestar el servicio de centro de operaciones de seguridad (security operation CENTER - SOC) y seguimiento de las operaciones de red para el monitoreo y respuesta a eventos de disponibilidad y seguridad	$ 323.330.096	Proceso adjudicado y celebrado
2024	SECRETARÍA DISTRITAL DE MOVILIDAD	SDM-PSA-MC-119-2024	Realizar la gestión y monitoreo de la seguridad informática sobre la plataforma tecnológica de la secretaría distrital de movilidad a través de un centro de operaciones de seguridad (SOC)	$ 942.875.253	Proceso adjudicado y celebrado
2023	GOBERNACION DE CALDAS	SAMC-SP-049-2023	Renovación del licenciamiento FORTINET y servicios de monitoreo de la plataforma (NOC + SOC) con el cual cuenta la Gobernación de Caldas, en las diferentes sedes de la entidad, garantizando de esta manera la protección a la red	$ 486.756.367	Proceso adjudicado y celebrado

Como se puede apreciar, los contratos se encuentran en SECOP II con objeto igual o similar y/o alcance relacionado con el requerido en el presente Estudio.

2. ANALISIS DE LA OFERTA

Debido a la naturaleza y las condiciones que se requiere, para el presente proceso contractual pueden participar tanto las personas Naturales o Jurídicas, que cumplan cada uno de las exigencias y requisitos de carácter jurídico y técnico solicitado por el INPEC a efectos de presentar su oferta y participar en el proceso Contractual. Para efectos de realizar el análisis de la oferta, se solicitó a diferentes Personas Naturales o Jurídicas que presten el servicio que el Instituto requiere, procediendo a remitir las especificaciones técnicas vía correo nstitucional a las siguientes compañías:

Entidades Invitadas a Participar en el Proceso

#	ENTIDAD	CORREO ELECTRÓNICO	Fecha de solicitud de la cotización por correo electrónico por parte del INPEC
1	CONVIEST SAS	gerenciadeproyectos@conviest.com	25-FEB-2026
2	CREAMOSLAB SAS	eloaiza@creamoslab.co	25-FEB-2026
3	E & C INGENIEROS SAS	alejandro.barrero@eycingenieros.com	25-FEB-2026
4	CONSEMAD	wilmer.galindo@consemad.com	25-FEB-2026
5	LAN SECURITY NETWORKS SAS	juan.castro@lsn.com.co	25-FEB-2026
6	RED COMPUTO LTDA	alatorre@redcomputo.com.co	25-FEB-2026
7	SPECTRA INGENIERÍA SAS	licitaciones2@spectra.com.co	25-FEB-2026
8	HIWARE	comercial@hiware.com.co	25-FEB-2026
9	RIT ENTERPRISE SOLUTIONS SAS	comercial@ritenterprise.com.co	25-FEB-2026
10	HARDWARE AND DESING	hardwareanddesing@gmail.com	25-FEB-2026

Luego de efectuar las solicitudes se recibieron las siguientes cotizaciones por parte de cuatro empresas, las cuales manifiestan el cumplimiento de los criterios técnicos, encontrándose exentas de IVA, se realizar un comparativo de las propuestas económicas, arrojando el resultado de análisis de precios que se resume en el siguiente cuadro:

CONSOLIDADO COTIZACIONES

DESCRIPCIÓN	UNIDAD DE MEDIDA	CONVIEST S.A.S	CREAMOSLAB S.A.S.	CONSEMAD S.A.S	E&C INGENIEROS	VALOR PROMEDIO UNITARIO EXCLUIDO DE IVA
SOLUCIÓN DE COMUNICACIÓN DE RED PARA EL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO – INPEC	1 UNIDAD	$ 401.604.400	$ 399.368.000	$ 398.169.800	$400.805.700	$ 399.986.975

Se observa que las variaciones no son tan altas, en tal sentido es posible estimar el presupuesto oficial de la contratación, con este presupuesto promedio la solución cubre la necesidad de la SOLUCIÓN DE COMUNICACIÓN DE RED PARA EL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO – INPEC, de acuerdo con el presupuesto oficial y es viable presupuestalmente adelantar el proceso de contratación.

DESCRIPCIÓN	CANTIDAD AJUSTADA	VALOR UNITARIO PROMEDIO	VALOR TOTAL ESTIMADO EXCLUIDO DE IVA	AFECTACIÓN CDP
SOLUCIÓN DE COMUNICACIÓN DE RED PARA EL INSTITUTO NACIONAL PENITENCIARIO Y CARCELARIO – INPEC	1	$ 399.986.975	$ 399.986.975	CDP: No. 45326 del 2026-02-20, por valor de $400.000.000, el cual se afectará hasta la suma de $399.986.975

En consecuencia, el valor estimado del proceso de contratación será hasta la suma de **TRESCIENTOS NOVENTA Y NUEVE MILLONES NOVECIENTOS OCHENTA Y SEIS MIL NOVECIENTOS SETENTA Y CINCO PESOS M/CTE ($399.986.975) Excluido de IVA**, incluidos los demás impuestos tasas o contribuciones a que haya lugar, así como los costos en que los proponentes puedan incurrir para la ejecución de la propuesta.

Proceso excluido de IVA, Fundamento Jurídico: art. 130 de la Ley 633 de 2000 y la certificación del Ministerio de Justicia y Derecho expedida para esta vigencia.

El presupuesto para el presente proceso se encuentra respaldado así:

El presupuesto oficial asignado para el presente proceso es hasta la suma de CUATROCIENTOS MILLONES DE PESOS M/CTE ($400.000.000), que se encuentra respaldado en el CDP No. 45326 del 2026-02-20, Unidad / Subunidad Ejecutora 12-08-00-000 INPEC-GESTION GENERAL, POSICIÓN CATÁLOGO DE GASTO C-1299-0800-7-40020112-1299085-02 MODERNIZACION INTEGRAL DE LAS CAPACIDADES TECNOLOGICAS DEL INPEC A NIVEL NACIONAL. ADQUIS, DE BYS-SERVICIOS TECNOLOGICOS, FUENTE: Nación, RECURSO: 10, SITUACIÓN: CSF. Objeto: BSITEM 909 SOLUCIÓN DE COMUNICACIÓN DE RED, OFICIO 20261E0037850 OFISI.

3. ANÁLISIS DEL RIESGO

El Instituto Nacional Penitenciario y Carcelario INPEC, identifica los siguientes riesgos asociados al proceso de contratación de conformidad La Ley 1150 de 2007; el artículo 4 de la Ley 80 de 1993; el artículo 25 numerales 7 y 12 y el artículo 2.2.1.1.1.6.3 del Decreto 1082 de 2015.

Tabla 5. Análisis del Riesgo

N°	1	2
Clase	General	Especifico
Fuente	Externo	Interno
Etapa	Ejecución	Ejecucion
Tipo	Riesgos sociales o políticos	Operacional
Descripción	Cambios en la política tributaria.	Fallas en la integración de la solución ofertada
Consecuencia de la ocurrencia del evento	Puedan afectar las utilidades esperadas o generar pérdidas	Pueden afectar la funcionalidad del sistema de protección de la red perimetral
Probabilidad	1	2
Impacto	3	2
Valoración	4	4
Categoría	Riesgo bajo	Riesgo bajo
¿A quién se le asigna?	Contratista / Entidad Estatal	Contratista
Tratamiento/Control a ser implementado	Verificación legal y Financiero sobre el contexto regulatorio en el cual se celebraría el contrato	Verificación de la ficha técnica y la funcionalidad del sistema.
Impacto después del tratamiento: Probabilidad	1	1
Impacto después del tratamiento: Impacto	3	1
Impacto después del tratamiento: Valoración	4	2
Impacto después del tratamiento: Categoría	Riesgo bajo	Riesgo bajo
¿Afecta la ejecución del contrato?	SI	SI
Responsable por implementar el tratamiento	Entidad Estatal	Contratista
Fecha estimada en que se inicia el tratamiento	Desde la celebración del contrato	Desde la celebración del contrato
Fecha estimada en que se completa el tratamiento	la liquidación del contrato	la liquidación del contrato
Monitoreo y revisión: ¿Cómo se realiza el monitoreo?	Análisis desde el punto de vista Legal y Financiero.	Verificación con el supervisor del contrato y equipo técnico del INPEC
Monitoreo y revisión: Periodicidad	Mensual	Permanente

3	Especifico	Interno	Ejecucion	Operacional	Incumplimiento en la ejecución del contrato	Afecta la gestión de la Entidad	1	5	6	Riesgo alto	Contratista	Establecer los requisitos técnicos y exigir una condición organizacional de recurso humano y técnico, experiencia, capacidad financiera, para que se presenten personas naturales y jurídicas capaces de cumplir el objeto del contrato	1	1	2	Riesgo bajo	SI	Grupo de Contratos	Ejecución del Contrato	Acta de Recibido a satisfacción	Revisión e inspección de la ejecución del contrato por parte del supervisor del contrato y el Grupo de Contratos	Permanente
4	Especifico	Externo	Ejecucion	Operacional	No suministrar la solución de red de acuerdo con el ofrecimiento de la oferta presentada	Incumplimiento del contrato	1	3	4	Riesgo bajo	contratista	Aclarar los requisitos, requerimientos y especificaciones del servicio. Hacer pruebas e inspecciones del servicio.	1	2	3	Riesgo bajo	SI	Supervisor del contrato	Ejecución del Contrato	Acta de Recibido a satisfacción	Inspección y revisión de la ejecución del contrato por parte del supervisor del contrato	Permanente
5	Especifico	Externo	Ejecución	Operacional	Baja calidad de la solución suministrada	Servicio de baja calidad	1	2	3	Riesgo bajo	contratista	Solicitar restablecimiento del servicio de comunicación.	1	1	2	Riesgo bajo	SI	Contratista	Ejecución del Contrato	Acta de Recibido a satisfacción	Inspección y revisión de la ejecución del contrato por parte del supervisor del contrato	Permanente

6	General	Externo	Ejecución	Económico	Se presenta fluctuación o incremento en los costos que afecten gravemente el cumplimiento del objeto y alcance del contrato	riesgo en las actividades programadas afectación utilidades esperadas se generan perdidas (variación valor comercial)	2	2	4	Bajo	Contratista	Verificación de los precios del mercado con el fin de determinar una posible modificación de los precios de referencia	1	1	2	bajo	si	Contratista	Estudios previos análisis del sector	Hasta la fecha de finalización del contrato	Se realiza con las cotizaciones y el análisis del sector	Etapa precontractual
7	General	Externo	Ejecución	Regulatorio	Se deriva de los efectos provenientes de las variaciones de las tasas de interés y de cambio, devaluación real y otras variables del mercado.	Puedan afectar las utilidades esperadas o generar pérdidas	1	3	4	Riesgo Bajo	Contratista	Verificación del Sector Económico y el impacto generado.	1	1	2	Riesgo Bajo	SI	Entidad Estatal	Inicio ejecución contractual	la liquidación del contrato	Análisis del Sector Económico y Financiero.	Mensual

8	General	Externo	Ejecución	Tecnológico	Vulnerabilidades de seguridad descubiertas post-implementación del objeto contractual	Afecta el funcionamiento de los servicios tecnológicos ofertados por la entidad	1	3	4	Riesgo Bajo	Contratista	Adquisición del servicio técnico por parte del contratista y del fabricante de la solución.	1	1	2	Riesgo Bajo	SI	Contratista	Inicio ejecución contractual	la liquidación del contrato	Verificación de actualizaciones a la última versión estable emitida por el fabricante	Permanente
9	General	Externo	Ejecución	Operacional	Incumplimiento en los plazos de entrega	Afecta la ejecución del contrato	2	3	5	Riesgo Medio	Contratista	Seguimiento al cronograma presentado por el contratista	1	2	3	Riesgo Bajo	SI	Contratista	Inicio ejecución contractual	la liquidación del contrato	Verificación del cronograma	Permanente

4. DECLARACIÓN DE RESPONSABILIDAD

En nuestra calidad de responsables de la Oficina de Sistemas de Información INPEC y de acuerdo con el trabajo realizado por el Grupo administración de las Tecnologías de la Información, en el cual se analizó la conveniencia, necesidad y estructuración de los estudios previos, para la realización de la contratación, con la suscripción de esta declaración manifestamos que es perentoria la realización de este proceso y por tal razón la única forma de resolver la necesidad es mediante la contratación propuesta, quedando evidenciada la necesidad del contrato tendiente a cumplir y satisfacer la necesidad institucional. Por consiguiente, se solicita adelantar el proceso contractual respectivo.

Atentamente,

Ingeniero GIOVANNY ZAMBRANO LONDOÑO
Jefe Oficina de Sistemas de Información

Revisó: Ingeniero Mario Rodríguez Medina – Coordinador Grupo Administración de las Tecnologías de la Información
Proyectó: Ing. Edwin Mauricio Romero – Grupo Administración de las Tecnologías de la Información
Fecha de elaboración: 27/02/2026