INPEC

ANÁLISIS DEL SECTOR

De conformidad con lo normado en el numeral 3 del artículo 5 de la ley 1150 de 2007 y de acuerdo con el Plan anual de adquisiciones del INPEC bajo el rubro A-02-01-01-006-002 PRODUCTOS DE LA PROPIEDAD INTELECTUAL, en coordinación con la Oficina de Sistemas de Información, se procede a realizar los siguientes Estudios Previos para **"ADQUISICIÓN DE HERRAMIENTA DE SEGURIDAD DE USUARIO FINAL"**

1. ASPECTOS GENERALES

La incorporación de una solución institucional de herramienta de seguridad para la protección de los usuarios finales reviste importancia estratégica para el Instituto Nacional Penitenciario y Carcelario (INPEC). En primer lugar, la continuidad operativa de la entidad depende de manera crítica de la integridad, disponibilidad y confidencialidad de sus sistemas tecnológicos. Plataformas como el Sistematización Integral del Sistema Penitenciario y Carcelario (SISIPEC), la gestión documental (GESDOC), el sistema de nómina y talento humano, los servicios de correo electrónico, entre otros, constituyen el núcleo de la operación penitenciaria moderna. Un incidente de malware, ransomware o ataque de ingeniería social dirigido contra los usuarios finales tiene la capacidad de comprometer estos servicios en cuestión de minutos, afectando la seguridad de los establecimientos de reclusión y poniendo en riesgo la protección de derechos fundamentales de la población privada de la libertad. Blindar a los usuarios frente a estas amenazas se traduce en preservar la estabilidad operativa y mitigar escenarios de riesgo que podrían escalar a incidentes de mayor impacto.

En un contexto de ciberamenazas crecientes, el INPEC no puede ser ajeno a la realidad de Colombia como uno de los países más atacados de la región: de acuerdo con el informe global de Fortinet, entre enero y noviembre de 2024 se registraron más de treinta y seis mil millones de intentos de ciberataque en el país. Las amenazas modernas no solo se centran en la infraestructura de red, sino que utilizan al usuario como vector primario de ataque, a través de phishing, troyanos, explotación de vulnerabilidades y ransomware. El impacto de un solo incidente de este tipo no se limita a la indisponibilidad de un servicio: puede derivar en pérdida o secuestro de información sensible, interrupción de procesos críticos, sanciones legales, litigios y un severo daño reputacional. La adopción de una solución de seguridad corporativa, con capacidades de detección y respuesta avanzada, actúa como un mecanismo de control que reduce drásticamente la probabilidad de materialización de estos riesgos y refuerza la posición institucional frente a entes de control y aseguradoras.

Desde la perspectiva financiera, la inversión requerida se sustenta en un análisis de costo–beneficio favorable. Estudios sectoriales muestran que el costo promedio de un ataque de ransomware a entidades públicas puede superar, en cuestión de horas, el valor de una herramienta de seguridad anual de soluciones de protección de usuarios finales. Los costos asociados —remediación, pago de horas extras al personal técnico, indisponibilidad de servicios, pérdida de productividad y eventual afectación reputacional— se traducen en montos sustanciales que, a mediano plazo, resultan muy superiores a la inversión inicial.

En este sentido, la herramienta de seguridad para usuario final opera como una póliza tecnológica cuyo retorno se materializa en la prevención de incidentes de alto costo y en la optimización del presupuesto TIC, al evitar reinversiones correctivas.

Otro factor determinante es la reducción de los tiempos de detección y respuesta ante incidentes. Sin una herramienta centralizada y moderna, la identificación de infecciones puede tardar días o semanas, tiempo durante el cual el malware puede propagarse por la red institucional. La herramienta de seguridad para usuario final inspecciona procesos en tiempo real, aplica heurísticas y análisis de comportamiento para diferenciar actividades legítimas de comportamientos maliciosos y activa mecanismos automáticos de contención casi inmediatos. De esta manera, se disminuye el Mean Time To Detect (MTTD) y el Mean Time To Respond (MTTR), dos indicadores clave de resiliencia operativa que fortalecen la confianza en los servicios digitales de la entidad.

Asimismo, la adquisición de esta tecnología responde a exigencias normativas y de política pública. La Resolución 500 de 2021 del Ministerio TIC adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI), obligando a cada entidad a demostrar la existencia de controles que garanticen la confidencialidad, integridad y disponibilidad de la información. Una herramienta de seguridad con consola de administración y capacidades de reporte forense brinda evidencia de cumplimiento de estos controles, facilita auditorías y permite mantener indicadores actualizados de riesgo residual. En la esfera internacional, la Organización de Estados Americanos y la ONU recomiendan a los Estados reforzar la protección de infraestructuras críticas de justicia y seguridad frente a malware y ciberataques, alineamiento que la presente iniciativa materializa.

La confianza tecnológica institucional también se ve reforzada. Un entorno digital protegido transmite la imagen de una entidad moderna y comprometida con la seguridad de la información pública. La percepción de protección incide tanto en los funcionarios como en la cooperación interinstitucional y la credibilidad ante organismos de control. Al blindar los dispositivos de los usuarios finales, el INPEC consolida su reputación como referente en buenas prácticas de ciberseguridad en el sector público colombiano.

La importancia de adquirir una herramienta de seguridad para usuario final radica en la convergencia de beneficios operativos, financieros, tecnológicos y normativos. Garantiza la continuidad de servicios penitenciarios esenciales, disminuye la exposición a riesgos institucionales, optimiza la utilización de los recursos públicos y refleja el compromiso de la entidad con la modernización y la excelencia en la gestión del riesgo digital. En un entorno donde las amenazas evolucionan de manera acelerada y el costo de la inacción se incrementa día a día, dotar al INPEC de capacidades de protección proactiva no es opcional, sino una condición para cumplir con su misión y salvaguardar la seguridad digital institucional y nacional.

1.1. ECONÓMICO

El Instituto Nacional Penitenciario y Carcelario (INPEC) administra un presupuesto anual de $2,16 billones de pesos para 2025, según la Resolución 00001 del 2 de enero de 2025, que aprobó la distribución de los recursos del Presupuesto General de la Nación[1]. En este marco, el Plan Anual de Adquisiciones reserva $300.000.000 pesos M/Cte para la adquisición de una herramienta de seguridad que proteja a los usuarios finales. A la TRM

[1] https://inpec.gov.co/documents/d/guest/r000001_02012025?download=true&utm

del 29 de agosto de 2025 ($4.019,09 COP/USD), dicho rubro equivale aproximadamente USD $74.643. Desde la perspectiva de las finanzas públicas, este monto representa apenas el 0,013 % del presupuesto institucional, pero protege procesos cuya indisponibilidad o corrupción de información puede generar pérdidas muy superiores a ese porcentaje.

La magnitud del riesgo se ilustra con la estadística de Cybersecurity Ventures[2], que calcula que los daños globales por ransomware alcanzarán los USD $275.000 millones anuales en 2031. En paralelo, IBM Security[3] reporta que el costo promedio de una filtración de datos en 2024 fue de USD $4,45 millones, con un 24 % de casos originados en endpoints sin protección adecuada. Si el INPEC llegara a enfrentar un solo incidente significativo de malware o fuga de información, el impacto financiero podría superar varias veces el valor de la inversión proyectada.

Aun en escenarios conservadores —como la afectación de un subconjunto de usuarios que derive en la indisponibilidad de sistemas por 24 horas— los costos en productividad, soporte y restauración de servicios se ubicarían por encima de USD $200.000, es decir, casi tres veces más del valor del proyecto. El factor diferencial está en la rapidez y efectividad de detección, herramientas de seguridad corporativas de última generación aseguran que más del 95 % de las amenazas se bloquean en tiempo real, reduciendo drásticamente la probabilidad de que se materialicen incidentes de alto impacto.

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

REGULATORIO

La contratación de una herramienta de seguridad para usuario final en el INPEC se sustenta en el marco jurídico de la contratación estatal colombiana. La Ley 80 de 1993 (Estatuto General de Contratación), la Ley 1150 de 2007 (medidas de eficiencia y transparencia), la Ley 1474 de 2011 (Estatuto Anticorrupción), las normas presupuestales y tributarias, así como las disposiciones cambiarias, constituyen el marco general de obligatoriedad. En particular, el artículo 25 de la Ley 80 exige la elaboración de estudios previos que acrediten necesidad, conveniencia, idoneidad y suficiencia de recursos, garantizando los principios de planeación, transparencia y economía del gasto público. El Decreto 1082 de 2015 reglamenta estos principios y en su artículo 2.2.1.1.2.1.1 establece el contenido mínimo de los estudios previos, incluyendo análisis de mercado, riesgos, especificaciones técnicas, modalidad de selección y fuentes de financiación.

En lo institucional, el Decreto 4151 de 2011 atribuye a la Oficina de Sistemas de Información la formulación y ejecución de la política TIC del INPEC, y la Resolución Interna 0243 de 2020 formalizó el Grupo de Administración de Tecnologías de la

[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

Información como dependencia responsable de diagnosticar necesidades y proyectar compras estratégicas de infraestructura tecnológica.

La Política de Gobierno Digital constituye el marco estratégico que obliga a que la información pública se ofrezca de forma segura, confiable y eficiente, premisa que exige sistemas de protección actualizados. La Resolución 500 de 2021 del MinTIC adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de dicha política, obligando a las entidades a implementar controles que aseguren la confidencialidad, integridad y disponibilidad de la información. Una herramienta de seguridad institucional cumple directamente con estos requerimientos, pues protege los equipos de los usuarios finales frente a amenazas que podrían comprometer servicios misionales.

A nivel internacional, organismos como la OEA y la ONU han recomendado reforzar la ciberseguridad en infraestructuras críticas de justicia y seguridad, marco en el cual se inscribe esta contratación.

En consecuencia, la decisión de invertir en una herramienta de seguridad para usuario final no responde únicamente a la conveniencia técnica, sino al cumplimiento expreso de mandatos legales, regulatorios 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 asignadas por el Decreto 4151 y la Resolución 0243, y (iv) proteger la infraestructura crítica penitenciaria frente a riesgos cibernéticos que comprometerían la seguridad nacional y los derechos fundamentales.

2. ANÁLISIS DE LA DEMANDA

2.1. Histórico de la Entidad

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

2.2. Análisis Intersectorial

Para realizar el análisis de precios, se consultó la página de SECOP II, revisando los contratos publicados que suscribieron otras entidades públicas con objeto igual o similar al requerido en el presente Estudio, relacionados en la siguiente tabla:

AÑO	ENTIDAD	No. CONTRATO	OBJETO	VALOR TOTAL DEL CONTRATO	ESTADO DEL PROCESO
2025	PERSONERÍA DE BOGOTÁ D.C	PB-SASI-2025-0006	RENOVACIÓN DE LAS LICENCIAS ANTIVIRUS PARA LA PERSONERÍA DE BOGOTÁ D.C	316.262.796	Proceso adjudicado y celebrado
2025	SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ	SGA-SASI-012-2025	ADQUIRIR UNA SOLUCIÓN DE PROTECCIÓN ANTIVIRUS DE NUEVA GENERACIÓN PARA LOS EQUIPOS DE CÓMPUTO DE LA SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE	291.625.100	Proceso adjudicado y celebrado

			BOGOTÁ D.C.		
2024	ARCHIVO GENERAL DE LA NACION	SASI-05-2024	ADQUIRIR LICENCIAMIENTO DE ANTIVIRUS PARA EL ARCHIVO GENERAL DE LA NACIÓN.	249.723.207	Proceso adjudicado y celebrado
2024	MINISTERIO DE TRANSPORTE	SASI-020-2024	RENOVAR EL LICENCIAMIENTO DE ENDPOINT ANTIVIRUS	380.000.000	Proceso adjudicado y celebrado

Como se puede apreciar, los contratos se encuentran en SECOP II con objeto similar.

3. Análisis 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 institucional a las siguientes compañías:

Entidades Invitadas a Participar en el Proceso

#	ENTIDAD	CORREO ELECTRÓNICO	FECHA DE SOLICITUD DE LA COTIZACIÓN POR CORREO ELECTRONICO POR PARTE DEL INPEC
1	ACONPIEXPRESS	aconpiexpress.com.co	12-AGO-2025
2	DASIELECTRONICOS	comercial@dasielectronicos.com	12-AGO-2025
3	LMDINGENIERIA	gcomercial@lmdingenieria.com	12-AGO-2025
4	PSS	edith.acevedo@pss.com.co	12-AGO-2025
5	SGT S.A.S	benjaminr@sgtsas.com	12-AGO-2025
6	I2SS	pedro.velez@i2ss.com	12-AGO-2025
7	RED COMPUTO	alatorre@redcomputo.com.co	12-AGO-2025

Luego de efectuar las solicitudes se recibieron las siguientes cotizaciones por parte de tres 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	I2SS	RED COMPUTO	PSS	VALOR PROMEDIO UNITARIO EXCLUIDO DE IVA
ADQUISICIÓN DE HERRAMIENTA DE SEGURIDAD DE USUARIO FINAL	1 herramienta de Seguridad para usuario final	$ 77.220	$ 77.700	$ 79.000	$ 77.973

Se evidencia que las variaciones de precio entre las ofertas analizadas no presentan diferencias significativas. En consecuencia, resulta viable establecer el presupuesto oficial de la contratación tomando como referencia el valor promedio unitario. Con base en dicho cálculo, se determina el número de herramientas de seguridad para usuario final requeridas para atender la necesidad descrita en el objeto contractual "ADQUISICIÓN DE HERRAMIENTA DE SEGURIDAD DE USUARIO FINAL". De esta manera, se concluye que el proceso cuenta con viabilidad presupuestal para ser adelantado:

UNIDAD DE MEDIDA	VALOR PROMEDIO UNITARIO EXCLUIDO DE IVA	VALOR ESTIMADO DEL PROCESO EXCLUIDO DE IVA
3,847 Herramientas de Seguridad para usuario final	$ 77.973	$ 299.962.131

En consecuencia, el valor estimado del proceso de contratación será hasta la suma de **DOSCIENTOS NOVENTA Y NUEVE MILLONES NOVECIENTOS SESENTA Y DOS MIL CIENTO TREINTA Y UN PESOS M/CTE ($299.962.131) 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 TRECIENTOS MILLONES DE PESOS M/CTE ($300.000.000), LEY 633 DEL 2000, que se encuentra

respaldado en el CDP: No. 69725 del 2025-07-30, Unidad / Subunidad Ejecutora 12-08-00-000 INPEC-GESTION GENERAL, POSICION CATALOGO DE GASTOS A-02-01-01-006-002 PRODUCTOS DE LA PROPIEDAD INTELECTUAL, FUENTE: NACIÓN. RECURSO 10, SITUACIÓN: CSF. ADQUISICIÓN DE HERRAMIENTA DE SEGURIDAD DE USUARIO FINAL. BSITEM 519. OFICIO 2025IE0145237.

4. 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 Análisis del Riesgo

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

2	Específico	Interno	Ejecución	Operacional	Fallas en la integración de la herramienta de Seguridad para usuario final ofertada	Pueden afectar la funcionalidad del sistema de protección del usuario final	2	2	4	Riesgo bajo	Contratista	Verificación de la ficha técnica y la funcionalidad de la herramienta de seguridad para usuario final	1	1	2	Riesgo bajo	SI	Contratista	Desde la celebración del contrato	la liquidación del contrato	Verificación con el supervisor del contrato y equipo técnico del INPEC	Permanente
3	Específico	Interno	Ejecución	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	Contratista	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 suministra la herramienta de seguridad de acuerdo con el ofrecimiento de la oferta presentada	Incumplimiento del contrato	1	3	4	Riesgo bajo	contratista	Aclarar los requisitos, requerimientos y especificaciones de la herramienta de seguridad. Hacer pruebas e inspecciones de la herramienta de seguridad.	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	Ejecucion	Operacional	Baja calidad de la herramienta de seguridad suministrado	Servicio de baja calidad	1	2	3	Riesgo bajo	contratista	Solicitar la entrega de la herramienta de seguridad original, vigente y verificable con el fabricante	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 a la entidad	1 3 4	Riesgo Bajo	Contratista	Adquisición del servicio técnico por parte del contratista y del fabricante de la herramienta de seguridad ofertada	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

5. 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: ING. Giovanny Zambrano Londoño – Jefe Oficina de Sistemas de Información
ING. Mario Rodríguez Medina – Coordinador Grupo Administración de las Tecnologías de Información
ING. Jhon Alexander Leal – Coordinador Grupo Seguridad Proyección e Implementación Tecnológica
Proyectó: ING. Edwin Mauricio Romero – Grupo Administración de las Tecnologías de la Información
Fecha de elaboración: 11/09/2025