INPEC

ESTUDIOS PREVIOS SELECCIÓN ABREVIADA POR SUBASTA INVERSA

1. DESCRIPCIÓN DE LA NECESIDAD.

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**"

Que el Decreto 4151 de 2011, establece las funciones de la Oficina de Sistemas de información en su artículo 12 y de conformidad con la Resolución Interna No. 0243 del 17 de enero de 2020, mediante la cual se desarrolla la estructura orgánica y se determinan los grupos de trabajo del Instituto Nacional Penitenciario y Carcelario (INPEC), el Artículo 19 establece el GRUPO DE ADMINISTRACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN como la dependencia encargada de gestionar la infraestructura tecnológica de la entidad. Dentro de sus funciones, dicho grupo debe identificar las necesidades tecnológicas del Instituto, proyectar y supervisar la adquisición de infraestructura a nivel nacional, así como administrar, mantener y actualizar las redes, equipos y sistemas de comunicación.

En este contexto, y atendiendo a la creciente necesidad de fortalecer las capacidades institucionales frente a ciberamenazas, se hace necesario resaltar lo siguiente:

Las amenazas digitales continúan incrementándose en complejidad, alcance y frecuencia, afectando de manera particular a entidades gubernamentales y organismos de seguridad del Estado. El INPEC, como infraestructura crítica de la Nación, administra información altamente sensible y depende de forma creciente de sistemas informáticos y servicios en línea para garantizar la operación penitenciaria, la seguridad de los establecimientos y la adecuada gestión de los procesos internos.

Según el reporte de ciberseguridad de Fortinet[1], Colombia registró más de 36.000 millones de intentos de ciberataques entre enero y noviembre de 2024, ubicándose entre los países más atacados de la región. Entre las amenazas más frecuentes se encuentran el malware, ransomware, phishing y ataques a dispositivos finales (endpoints), los cuales representan un riesgo directo para la confidencialidad, integridad y disponibilidad de la información institucional.

Los funcionarios del INPEC, realizan sus labores mediante equipos de cómputo y dispositivos conectados a la red institucional, accediendo a plataformas como SISIPEC, GESDOC, correo institucional, aplicativos financieros, recursos educativos virtuales, sistemas de gestión administrativa, en otros. Cada uno de estos usuarios finales representa un punto de entrada potencial para atacantes que buscan comprometer la seguridad de la institución.

La seguridad perimetral implementada en el INPEC constituye una primera línea de defensa frente a múltiples amenazas externas; sin embargo, el panorama actual de ciberseguridad exige un enfoque integral que también proteja a los usuarios finales como posibles vectores de ataque. En este sentido, la implementación de la herramienta seguridad avanzado se convierte en un complemento indispensable para fortalecer la defensa en profundidad del ecosistema digital institucional, garantizando una cobertura que abarca tanto el perímetro como los equipos de cómputo utilizados en la operación penitenciaria y administrativa.

Esta herramienta de seguridad permitirá:

[1] Informe de Fortinet: Los actores de amenazas apuntan cada vez más hacia las organizaciones de OT, https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2024/fortinet-report-threat-actors-increasingly-targeting-ot-organizations

- Prevenir y mitigar infecciones por malware, ransomware, troyanos y software espía.
- Contar con detección y respuesta en tiempo real frente a comportamientos anómalos en los equipos de usuario final.
- Generar reportes centralizados de incidentes de seguridad para la gestión proactiva de amenazas.
- Facilitar actualizaciones automáticas y permanentes que garanticen la vigencia frente a nuevas amenazas.
- Proteger la confidencialidad de la información administrativa y penitenciaria almacenada o procesada en equipos de la entidad.

Adicionalmente, organismos internacionales como la ONU y la OEA[2] han instado a los Estados a robustecer la ciberseguridad en instituciones de justicia y seguridad. En Colombia, la Política de Gobierno Digital y la Resolución MinTIC 500 de 2021[3], que adopta el Modelo de Seguridad y Privacidad de la Información (MSPI), establecen la obligación para las entidades públicas de implementar controles que fortalezcan la protección de sus activos digitales, incluyendo medidas directas en el nivel de usuarios finales.

El Grupo de Administración de Tecnologías de la Información del INPEC ha identificado que actualmente la entidad no cuenta con una solución institucional de seguridad para los usuarios finales. Esta situación genera la necesidad de implementar un sistema centralizado y robusto de protección que acompañe el crecimiento de la red y responda a la evolución de las amenazas cibernéticas, con el fin de mitigar riesgos operativos, legales y reputacionales, y garantizar la continuidad y seguridad de los servicios tecnológicos del Instituto.

En conclusión, la adquisición de la herramienta de seguridad para la protección de los usuarios finales representa una necesidad prioritaria y estratégica para el INPEC, en tanto:

- Garantiza la seguridad digital de los funcionarios y dependencias administrativas.
- Asegura la continuidad operacional de los servicios tecnológicos penitenciarios y administrativos.
- Cumple con la normativa nacional en materia de seguridad digital.
- Fortalece las capacidades institucionales frente a un panorama de amenazas cada vez más complejo.

Con ello, el Instituto avanza en la consolidación de un ecosistema de ciberseguridad integral, protegiendo sus activos digitales, garantizando la prestación de servicios tecnológicos de forma confiable y contribuyendo al cumplimiento misional del sistema penitenciario colombiano.

Por lo tanto, se establece la necesidad prioritaria de adquirir una herramienta de seguridad para garantizar la protección de los usuarios finales en los establecimientos penitenciarios y dependencias administrativas, fortaleciendo la seguridad de los servicios tecnológicos institucionales tales como SISIPEC, correo electrónico, GESDOC, Humano, entre otros, y reduciendo el riesgo de incidentes que comprometan la continuidad y disponibilidad de la operación del INPEC.

2. OBJETO A CONTRATAR CON SUS ESPECIFICACIONES

2.1 OBJETO DEL CONTRATO

ADQUISICIÓN DE HERRAMIENTA DE SEGURIDAD DE USUARIO FINAL

[2] Organización de los Estados Americanos OEA, Programa de Ciberseguridad. https://www.oas.org/ext/es/seguridad/prog-ciber

[3] https://mintic.gov.co/portal/715/articles-2627_Resolucion_2239_de_2024.pdf?utm

2.2 ESPECIFICACIONES TECNICAS MÍNIMAS SOLICITADAS

ÍTEM	ADQUISICIÓN DE HERRAMIENTA DE SEGURIDAD DE USUARIO FINAL
Especificar	Marca: Especificar
	Modelo: Especificar
1.	La solución que se implementa en dispositivos Endpoint debe evitar ataques de malware basados en archivos, detectar actividades maliciosas y proporcionar las funciones de investigación y corrección necesarias para responder a incidentes y alertas de seguridad dinámicas.
1.1	Debe ofrecer una protección avanzada con un motor de detección optimizado, capaz de identificar amenazas en tiempo real, manteniendo un impacto mínimo en el rendimiento del sistema y un bajo consumo de CPU y RAM, en idioma español. Se debe entregar la última versión estable emitida por el fabricante.
1.2	La solución de Endpoint debe estar disponible y soportada para los siguientes sistemas operativos: Sistemas operativos de escritorio: • Microsoft Windows 11, 10 Sistemas operativos de servidor: • Microsoft Windows Server 2025, 2022, 2019, 2016, 2012 R2 Sistemas operativos Linux: • Ubuntu, RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server, Rocky Linux, Amazon Linux y Oracle Linux Sistemas operativos Mac OS: • Mac OS Big Sur (11) hasta macOS Sequoia (15) Sistemas operativos para Smartphones y tablets • Android 9 y superior • iOS 11 y superior
1.3	Debe ser compatible con los siguientes entornos virtuales • VDI (Virtual Desktop Infraestructura) • VMware • Citrix

1.4	La herramienta de seguridad de usuarios finales deberá contar con las siguientes funcionalidades • Antivirus y Antispyware • Navegador Seguro • Motor reputacional • Motor Heurístico • Protección contra amenazas a través de la protección proactiva • Machine learning • Protección contra Botnet • Bloqueador de Exploit • Escaner avanzado de memoria • Protección Web • Protección contra ataques en la red (IDS) • Firewall bidireccional • Protección antispam • Sistema de prevención de intrusiones basado en el host (HIPS) • Control Web • Control de dispositivos
1.5	La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso, priorizando el rendimiento del usuario.
1.6	Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.
1.7	Tener la Capacidad en tiempo real de explorar, detectar, remover, limpiar, aislar, proteger y borrar virus existentes tanto en memorias, discos, disquetes, unidades de almacenamiento USB, unidades de red y cualquier otro medio por el cual sea posible la replicación de virus, o residente en memoria. Debe contar con un sistema de alertas el cual notifique los procesos de escaneo, limpieza e infecciones de los usuarios y notificarlos a la consola de administración.
1.8	La solución en cada estación debe tener integrados los módulos de antivirus, antispyware, para la detección de amenaza como virus, spyware, adware, gusanos, rootkits, phishing, aplicaciones peligrosas, aplicaciones indeseables. Capacidad de remoción para virus binarios, troyanos, gusanos y archivos descargados con contenido malicioso. Capacidad de protección contra códigos potencialmente hostiles, tales como ActiveX, Applets, aplicaciones Java, JavaScript, otras vulnerabilidades, etc.
1.9	La protección contra botnet debe detectar y bloquear las comunicaciones maliciosas de C&C y procesos dañinos, mediante el análisis de los patrones de las comunicaciones y los protocolos de la red.
1.10	La solución debe estar en capacidad de detectar códigos potencialmente sospechosos, independientemente de si se encuentran en el disco o en los procesos activos de memoria, así como identificar muestras de malware aún desconocido. Igualmente debe utilizar DNA Detections – detección basada en "genes" del malware.
1.11	La solución debe ser capaz de brindar protección contra ataques de red, debe analizar el contenido del tráfico de red y realice la detección de las vulnerabilidades conocidas en el nivel de la red.
1.12	La solución deberá contar con módulo de exploración avanzada de memoria que permita detectar comportamiento sospechoso y buscar amenazas cuando se manifiestan en la memoria del sistema.
1.13	La solución debe contar con la protección de banca para pagos en línea la cual asegura que todas las transacciones en línea se encuentren protegidas dentro de un entorno seguro y confiable.

1.14	El motor de protección de la herramienta de seguridad para usuarios finales debe contar con un componente avanzado de aprendizaje automático que mejora la detección del malware en función del aprendizaje, lo que permite identificar malware nuevo sin depender exclusivamente de firmas tradicionales.
1.15	El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.
1.16	Deberá tener la capacidad para aplicar durante cierto periodo de tiempo las reglas de control de dispositivo y de control de acceso web a través de la consola de administración.
1.17	El bloqueo restricción de acceso web deberá poder asignarse, por grupo y por equipo.
1.18	La solución deberá permitir excluir determinados sitios web para que no sean bloqueados.
1.19	Deberá tener la capacidad de enviar una tarea para la actualización de los parches del sistema operativo.
1.20	Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.
1.21	La herramienta de seguridad para usuario final debe ejecutar un escaneo únicamente en los siguientes estados en la estación de trabajo: • Protector de pantalla activo • Sesión de usuario bloqueada • Sesión de usuario finalizada
1.22	La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los siguientes criterios: • Fabricante • Modelo • Número de serie
1.23	La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar únicamente de los siguientes permisos: • Lectura/Escritura • Bloqueo • Solo de lectura • Advertir
1.24	El módulo de control de dispositivos debe soportar los siguientes medios: CD/DVD/Blu-ray, medios de almacenamiento USB, Dispositivos FireWire, Impresora USB, Bluetooth, Lectores de tarjetas, Módem, Puertos LPT/COM.
1.25	El módulo de control de dispositivos debe permitir crear reglas basadas en tiempo
1.26	El análisis automático debe permitir analizar dispositivos y medios extraíbles en busca de malware apenas se inserten en el equipo y debe incluir UEFI Scanner – protección a nivel de firmware antes del arranque.
1.27	Al conectar o usar un dispositivo de almacenamiento, la herramienta de seguridad para usuario final debe proporcionar las siguientes opciones: • Escanear • No realizar ninguna acción • Recordar esta acción

1.28	La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema (HIPS) debe tener los siguientes modos de configuración: • Modo automático • Modo inteligente • Modo interactivo • Modo política • Modo aprendizaje
1.29	El aprendizaje automático avanzado o "machine learning" deberá tener cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado. Igualmente debe utilizar Advanced Machine Learning offline – IA local que funciona sin internet.
1.30	Debe permitir definir reglas para las claves de registros, procesos, aplicaciones y archivos del sistema. Proporcionando protección contra la manipulación del sistema.
1.31	La herramienta de seguridad para usuario final debe contar con un módulo de protección que permita proteger el sistema UEFI/sectores de arranque de los equipos, ante la carga de código malicioso del tipo bootkits UEFI que afecten la capa del firmware del sistema.
1.32	El módulo de HIPS debe incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro.
1.33	La protección Antiexploits debe monitorea aplicaciones explotables (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java y más), y se activa, la amenaza se esta debe ser bloqueada inmediatamente en la máquina.
1.34	La protección contra ransomware, debe monitorear y evaluar todas las aplicaciones ejecutadas en base a su comportamiento y reputación. Debe detectar y bloquear procesos que se asemejan al comportamiento del ransomware.
1.35	Debe contar con un módulo de protección de correo que permita filtrar y mantener libre de SPAM a los clientes de correo.
1.36	La solución debe contar con un módulo antispam dedicado que permita explorar los correos entrantes y de esta manera filtrar y/o eliminar automáticamente el correo electrónico no deseado.
1.37	El módulo antispam debe permitir la creación de listas blancas y negras de direcciones de correos o dominios que se van a bloquear o a permitir, que se puedan crear de forma individual para cada cliente o grupo.
1.38	La solución debe capaz de verificar las comunicaciones usando protocolos SSL para hallar amenazas.
1.39	Debe contar con un sistema que permita comprobar la reputación de los procesos en ejecución y los archivos directamente desde cliente, lo cual permita reaccionar de forma inmediata ante amenazas más recientes.
1.40	Al aparecer una amenaza 0-day, el archivo debe enviarse a un sistema de protección contra malware basado en la nube, donde se activa la amenaza para monitorear su comportamiento. Los resultados deben distribuirse a todas las endpoints a nivel mundial en cuestión de minutos, sin requerir ninguna actualización.
1.41	Debe monitorear las aplicaciones que suelen ser atacadas por exploits con mayor frecuencia (navegadores, lectores de documentos, clientes de correo electrónico).
1.42	Debe detectar y bloquear ataques automáticos o DDOS, que intentan usar técnicas de adivinación de contraseñas para obtener acceso a su red.

1.43	La herramienta de seguridad para usuario final debe contar con un firewall a nivel de Host. El firewall debe tener los siguientes modos de configuración: • Modo automático • Modo interactivo • Modo basado en políticas • Modo aprendizaje
1.44	Las reglas de firewall creadas deberán ser capaces de permitir las siguientes acciones de filtrado: • Denegar • Permitir • Preguntar
1.45	Debe permitir la creación de reglas de forma manual y automáticamente; especificando parámetros del socket de origen y destino, protocolo y aplicación utilizada.
1.46	Debe bloquear las conexiones no autorizadas (entrantes o salientes) a los ordenadores de la entidad o configurarlas desde el editor de reglas.
1.47	Debe permitir agregar información de redes o subredes diferentes a la propia, con el fin de habilitar servicios fuera de ella.
1.48	La solución debe ser capaz de realizar la detección de redes de confianza, proporcionando una protección rigurosa cuando los clientes se conectan a una red nueva, red pública o no autorizada.
1.49	El módulo debe detectar las zonas de confianza que permite identificar las zonas de red confiables por medio de las configuraciones de red, como la dirección IP del servidor principal / DNS / DHCP, red inalámbrica SSID.
1.50	Debe contar con Sistema de Detección de Intrusiones, que analiza el contenido del tráfico de red y le protege contra posibles ataques de red
1.51	Monitor en tiempo real de procesos en ejecución y clasificación de seguridad de cada uno de ellos, carga de operaciones sobre el sistema de archivos, procesos y servicios en ejecución
1.52	Debe contar con un monitor que muestre la descripción de la lista de procesos y aplicaciones que se comunican a través de la red, el protocolo de navegación (TCP o UDP), así como la dirección remota a la que se conecta la aplicación. Suministrando información como: protocolo, dirección Local, dirección remota, puerto local y remoto.
1.53	Debe incluir Herramientas de diagnóstico del equipo que muestren en detalle las configuraciones de procesos y servicios en ejecución, aplicaciones, estado e información de hardware, archivos esenciales de sistema operativo, Revisiones y actualizaciones, log de eventos y sistema (S.O.) etc.
1.54	La herramienta de diagnóstico debe ser capaz de realizar un análisis en profundidad del sistema del equipo para identificar posibles riesgos de seguridad y rastrear la presencia de código malicioso.
1.55	Capacidad de crear archivos de volcado de memoria, para futuras tareas diagnósticas acerca del rendimiento de la herramienta de seguridad para usuario final en el equipo.
1.56	Debe incluir un módulo que permita envió de muestras de malware no reconocido a laboratorio para su análisis
Protección para Servidores	
2.1	Contar con un producto para servidores con protección avanzada con tecnologías de machine learning, análisis de comportamiento y análisis de reputación para identificar archivos y comportamientos sospechosos, con bajo impacto de rendimiento en el sistema.

2.2	Debe contar con una versión diseñada especialmente para entornos de Servidor Windows o Linux, que ofrezca una solución efectiva contra ataques de malware y proporcionar protección: Antivirus y antispyware.
2.3	La solución de servidores para Linux deberá funcionar con las distribuciones Linux de código abierto usadas con mayor frecuencia y más recientes
2.4	La solución de servidores deberá contar con las siguientes funcionalidades • Antimalware • Machine learning • Protección contra Botnet • Bloqueador de Exploit • Escáner avanzado de memoria • Protección contra ransomware • Protección contra ataques en la red (IDS) • Firewall bidireccional • Protección del acceso a la Web • Sistema de prevención de intrusiones basado en el host (HIPS) • Protección contra phishing
2.5	Debe contar con una tecnología que permite explorar discos de máquina virtual (VM) en Microsoft Hyper-V Server sin necesidad de ningún "agente" en la máquina virtual específica.
2.6	La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.
2.7	Debe contar con la opción o funcionalidad de aislar de la red el servidor, es decir bloquear todo el tráfico de red. Debe poderse ejecutar esta acción vía consola o línea de comandos.
2.8	La solución debe prevenir ataques por fuerza bruta, inspecciona el contenido del tráfico de red y bloqueando ataques para adivinar contraseñas de los servicios RDP y SMB
2.9	Debe permitir limitar conexiones RDP entrantes, permitiendo restringir las conexiones RDP en un conjunto de IP en una Zona de confianza.
2.10	Contar con protección a nivel de red, que mantenga las comunicaciones en el servidor Windows bajo control al habilitar un módulo de firewall para entornos de servidor.
2.11	La solución deberá agregar de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor.
2.12	Protección de botnets que detecte la comunicación maliciosa utilizada por botnets, identificar los procesos sospechosos y comprometidos, la comunicación maliciosa detectada debe ser bloqueada.
2.13	Debe optimizar el rendimiento de infraestructuras mixtas (hardware y virtuales) siendo capaz de eliminar la duplicidad de exploraciones en archivos, excluyendo los archivos ya explorados y limpios.
2.14	Debe contar con una capa adicional que protege a los usuarios del ransomware. Esta tecnología monitorea y evalúa todas las aplicaciones ejecutadas en función de su comportamiento y reputación diseñada para detectar y bloquear los procesos con un comportamiento similar al del ransomware.
Consola de Gestión	
3.1	La consola de administración debe poder implementarse en la nube o de forma local, que garantiza visibilidad en tiempo real de los equipos locales y externos, así como la elaboración de informes completos y gestión de la seguridad para todos los sistemas operativos.

3.2	La consola de acceso al servidor deberá ser 100% web, para ser accedida desde cualquier punto de la red utilizando un navegador de páginas de Internet como Internet Explorer, Mozilla Firefox, Google Chrome.
3.3	La consola de administración debe ser única para todas las funcionalidades solicitadas y debe administrar todos los dispositivos incluido dispositivos móviles iOS y Android.
3.4	La consola debe poder instalarse en forma de Appliance y debe soportar alguna de las siguientes plataformas de virtualización. • VMWare vSphere • Oracle Virtual Box • Microsoft Hyper-V • Azure – ambiente en la nube
3.5	La consola debe controlar y administrar todas las soluciones de seguridad del fabricante implementadas en la red, incluyendo estaciones de trabajo, servidores, máquinas virtuales e incluso dispositivos móviles gestionados.
3.6	La consola deberá permitir agregar, registrar equipos utilizando al menos los siguientes métodos: Sincronización con Active Directory, Ingreso de nombre o dirección IP del equipo de manera manual, Tecnología propia para la detección de equipos.
3.7	Debe permitir activar el doble factor de autenticación para el acceso a la consola, deber estar integrada a la misma consola, sin ningún ADD-ON o software adicional.
3.8	Debe permitirse crear varios usuarios y grupos de permisos para limitar el acceso a la consola de gestión. La consola debe contar con un sistema avanzado de control de acceso basado en roles (RBAC)
3.9	Luego de intentos no satisfactorios de inicio de sesión desde una misma dirección IP, la consola deberá bloquear de forma temporal los intentos posteriores de esta dirección IP por 10 minutos.
3.10	La consola deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.
3.11	Debe permitir generar grupos de clientes dinámicos y grupos estáticos.
3.12	Administrador de directivas que permita asignar automáticamente políticas de configuración a los clientes de acuerdo con los grupos estáticos, dinámicos o de forma individual
3.13	Lo grupos dinámicos deben permitir incluir reglas de tiempo, para que los equipos apliquen políticas o reglas durante el periodo de tiempo especificado.
3.14	Deberá contar con etiquetas independiente al LDAP, para identificar y buscar objetos similares.
3.15	Debe mostrar información básica del cliente (sistema operativo, configuración de hardware, software o aplicaciones instaladas, IP, usuarios autenticados, Número de amenazas sin resolver, Última conexión).
3.16	La consola debe permitir forzar la configuración de los módulos de protección, que active o desactive de los módulos de manera permanente en el cliente.
3.17	Debe permitir la funcionalidad de aislar de la red el equipo o servidor, es decir bloquear todas las conexiones, excepto las que sean necesarias con la consola de gestión
3.18	La solución debe permitir desde la consola de administración realizar la exclusión de la exploración de procesos en todo el sistema basadas en hash checksum de un archivo.
3.19	Debe de contar con un desinstalador de herramientas de seguridad de terceros.
3.20	La interfaz web de la consola deberá trabajar con paneles informativos que sean totalmente interactivos, los cuales permitan ver Información general del estado de la solución y múltiples pestañas con información.

3.21	Los paneles informativos de la interfaz gráfica podrán ser modificados por el administrador en tiempo real.
3.22	La interfaz web deberá trabajar con múltiples pestañas y deberá permitir la creación manual de más pestañas si es que el administrador lo requiere.
3.23	Debe contar con módulos específicos o asociados a las estadísticas generadas por las estaciones de trabajo de acuerdo con elementos específicos de la herramienta de seguridad para usuario final (Módulo de eventos, infecciones, alertas de firewall, cuarentena, antispam, filtros web, control de dispositivos de almacenamiento, exploración). Proporcionando registros completos e informes de todos los eventos relacionados.
3.24	Obtener a través de la consola de administración de seguridad del punto final inventario de aplicaciones y de hardware de cada uno de los equipos protegidos y la recopilación de eventos o detecciones en los equipos.
3.25	Debe manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los puntos finales e integrarse con la solución de detección y respuesta del punto final.
3.26	La consola de administración debe tener la capacidad para construir ambientes distribuidos donde pueda asignarse roles independientes a cada componente, así tener un componente diferente para: • Administrador de equipos móviles • Distribuidor de actualizaciones, paquetes de instalación y reenvío de comunicación entre el punto final y el servidor • Detector de puntos finales no administrados
3.27	La consola debe poder realizar la Instalación del producto de manera remota de todas las soluciones de seguridad de manera transparente y desatendida para el usuario.
3.28	La solución debe permitir la distribución o instalación del agente mediante políticas de GPO.
3.29	La consola debe permitir los siguientes aspectos: • Ejecutar tareas en periodos aleatorios y automáticas. • Crear y personalizar paquetes con diferentes configuraciones. • Desplegar de forma remota paquetes de instalación de la herramienta de seguridad para usuario final en segundo plano, sin intervenir las labores del usuario y sin reiniciar el equipo. • Definir tiempos programables.
3.30	La solución debe tener el mecanismo para desinstalar otras herramientas de seguridad presentes en el equipo final. Este mecanismo debe ser y estar: • Integrado al paquete de instalación de la solución de protección de punto final • Disponible solamente a través de la misma consola de administración de protección al punto final.
3.31	Debe minimizar el consumo de ancho de banda de la entidad descargando actualizaciones solo una vez a un repositorio local de actualizaciones y replicarlas a todos los equipos de la red.
3.32	En la consola de administración, se podrán administrar, configurar y aplicar políticas relacionadas a funcionalidades del dispositivo.
3.33	Módulo de reportes que permita generar información estadística sobre las alertas generadas por las estaciones de trabajo.
3.34	El módulo de reportes debe contar con plantillas de reportes de uso regular por administradores y de igual manera debe permitir la creación de plantillas nuevas, basadas en los criterios que el administrador considere importantes.

3.35	Los reportes deben tener la capacidad de generarse automáticamente y ser enviados a cuentas de correo electrónico. Debe permitir seleccionar entre varios formatos de archivo de salida con formatos como PDF o CSV.
3.36	Lo reportes podrán ser enviados automáticamente por correo electrónico o almacenados en el servidor según lo requiera el administrador.
3.37	Permitir desde la consola de administración, la gestión de actualizaciones sobre el sistema operativo.
3.38	Debe ser compatible con las herramientas SIEM y poder generar toda la información de registro en el formato JSON o LEEF, que permita la integración con Centros de Operaciones de Seguridad (SOC).
3.39	Debe contar con un módulo de MDM, que permita inscribir y gestionar desde la consola centralizada este tipo de dispositivos, desde allí, se podrán realizar configuraciones para los equipos sincronizados.
Remediación de Ransomware	
4.1	Debe contar con un módulo de remediación de Ransomware, que permita poder restaurar automáticamente los archivos cifrados cuando se detecta ransomware en una fase posterior del ataque, una vez que el proceso de cifrado ya ha comenzado.
4.2	El módulo de remediación de Ransomware debe crear una copia temporal segura del archivo, cuando se detecta posibles detecciones de comportamientos anómalos de cifrado.
4.3	El módulo debe proporcionar una restauración completa y automatizada de archivos a partir de copias de seguridad seguras.
4.4	Debe contar con su propia y exclusiva tecnología patentada y no ser basada en la función VSS (Volume Shadow Copy Service) de los sistemas operativos Windows de Microsoft.
4.5	Debe permitir a los administradores de la solución poder configurar las carpetas protegidas y los tipos de archivos protegidos. Archivos protegidos tales como mp3, 7z, pkg, rar, zip,csv, dat, sql, xml, bat, bin, gif, jpeg, jpg, png, html, ppt, pptx, java, xls, xlsx, mp4, doc, docx, pdf, txt.
Protección para dispositivos móvil	
5.1	La protección para dispositivos móviles debe cubrir los dispositivos Android
5.2	La herramienta de seguridad para usuario final debe realizar análisis a las aplicaciones instaladas, archivos. DEX.
5.3	La herramienta de seguridad para usuario final ofertado deberá analizar memoria interna y tarjeta SD para cualquier tipo de archivo.
5.4	Debe mostrar un listado de las aplicaciones instaladas, controlar el tiempo del uso de aplicaciones y tener el detalle de los permisos que usan los aplicativos del dispositivo móvil.
5.5	La protección del dispositivo móvil debe contar con una protección en tiempo real, además de contar con un sistema de reputación de archivos.
5.6	Deberá poder administrar las aplicaciones que deberían estar instaladas en los dispositivos móviles.
5.7	Debe tener la capacidad para detectar de forma automática aplicaciones no deseadas y no seguras para usar en el dispositivo móvil.
5.8	La solución debe poder enviar mensajes SMS al administrador cuando existen usuarios no autorizados manipulando el dispositivo móvil.
5.9	La solución será capaz de proteger y seleccionar los navegadores a usar.

5.10	La herramienta de seguridad para usuario final deberá ser inteligente para optimizar la batería del dispositivo y ejecutar el análisis al dispositivo únicamente cuando esté completamente cargado o conectado a la energía eléctrica.
5.11	La solución será capaz de detectar nuevas tarjetas SIM instaladas en el dispositivo y bloquearlas.
5.12	Es importante que la solución sea capaz de generar códigos de verificación SMS temporales al administrador para ejecutar tareas de desbloqueo de dispositivos o regresar a configuración de fábrica.
5.13	La solución será capaz de mantener un control de aplicaciones, bloquearlas según los permisos de la aplicación o por categoría, deberá limitarse a instalar aplicaciones únicamente desde Google Play, y poder bloquear cualquier aplicación en el momento que se necesite.
5.14	La solución será capaz de evitar ataques de suplantación de identidad de sitios web.
5.15	La protección móvil debe permite cubrir dispositivos con sistema operativo IOS como dispositivos Iphone, Ipad y llevar a cabo ciertas configuraciones y gestión de acuerdo con el alcance de la solución.
5.16	Tener la capacidad de crear listas blancas/negras, para evitar que usuarios realicen instalaciones de softwares o aplicaciones que no están permitidas dentro de la organización.
5.17	Debe realizar el filtrado de contenido web a nivel de categoría sobre contenido de adultos, (Definido por Apple), así mismo, lista de URL definidas por el administrador de la consola.
5.18	Permitir a los administradores de dispositivos gestionar diversas funciones de sincronización, almacenamiento y seguridad de datos en iCloud para los usuarios.
Protección basada en la nube	
6.1	Debe contar con un módulo con tecnología proactiva que utilice análisis adaptativo avanzado, inteligencia artificial de vanguardia, Sandbox en la nube y análisis de comportamiento en profundidad para prevenir ataques dirigidos,
6.2	Debe hacer uso de Sandboxing en la nube para analizar el comportamiento de archivos.
6.3	Debe brindar protección proactiva contra amenazas 0-day mediante la ejecución de las muestras sospechosas enviadas a un entorno aislado de sandboxing en la nube, con el fin de evaluar su comportamiento. De igual forma debe usar un sistema global de reputación en la nube.
6.4	Debe permitir crear una exclusión por ruta, tipo de detección y su hash (SHA-1).
6.5	Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.
6.6	Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.
6.7	Debe tener la capacidad para enviar correos SPAM para su análisis.
6.8	Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.
6.9	Debe tener la siguiente información de un archivo enviado al Sandboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.
6.10	Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.
6.11	Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.

6.12	Debe tener la capacidad de poder enviar un archivo/ejecutable a través de una consola de administración del punto final.
6.13	Debe permitir la configuración detallada de políticas por equipo, de modo que el administrador puede controlar lo que se envía y lo que debe ocurrir en función del resultado recibido.
Protección de cifrado de disco	
7.1	Debe permitir a los administradores implementar, activar y administrar el cifrado del disco del sistema, particiones o unidades completas en los equipos con un solo clic.
7.2	El cifrado de disco completo debe cifrar el sistema de discos, particiones y unidades completas para garantizar que todo lo almacenado en cada equipo o portátil está bloqueado y seguro, protegiéndote contra la pérdida o robo de esta información
7.3	La tecnología de cifrado de disco debe estar validada por FIPS 140-2 con cifrado AES de 256 bits, acelerado por hardware, que garantiza un cifrado y descifrado rápido y eficiente con un impacto mínimo en el rendimiento del sistema.
7.4	La solución deberá ser capaz de cifrar los equipos con sistemas operativos Windows y MacOS (FileVault) desde un solo panel.
7.5	Para equipos con sistema operativo Windows, debe tener una opción sobre activación de inicio de sesión único (SSO) para el ordenador del usuario.
7.6	La solución de cifrado debe permitir usar una contraseña de inicio de sesión de la estación de trabajo
7.7	La solución de cifrado debe permitir anular la contraseña de inicio de sesión de la estación de trabajo
7.8	El administrador podrá establecer requisitos de contraseña obligatorios, la cantidad de reintentos y el período de vencimiento. Desde la configuración de las políticas debe ser posible otorgar a un usuario la opción de cambiar su contraseña cuando lo desee.
7.9	La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.
7.10	La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.
7.11	La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones.
7.12	Desde la consola de gestión, el administrador podrá emitir el proceso de cifrado de una máquina final, donde el administrador podrá asignar la llave simétrica, evaluar el progreso y comportamiento del cifrado de la máquina, para que el usuario final no deba intervenir y así mitigar riesgos.
Protección de aplicaciones en la nube (Microsoft y Google Workspace)	
8.1	Proporcionar una protección avanzada para las aplicaciones de Microsoft y Google Workspace (Exchange Online, OneDrive, Teams, SharePoint Online, Gmail, Google Drive) contra malware, spam o ataques de phishing con la máxima defensa contra amenazas 0-day.
8.2	Debe brindar protección con defensa proactiva contra amenazas para el correo electrónico en la nube, con análisis antimalware, filtrado de spam, antiphishing, antispoofing y defensa avanzada contra amenazas con sandboxing en la nube, que ayuda a proteger las comunicaciones y el almacenamiento en la nube de su entidad.
8.3	Estar en la capacidad de analizar los correos electrónicos entrantes y sus archivos adjuntos, así como todos los archivos nuevos y modificados, evitando la propagación de malware a través del almacenamiento en la nube en múltiples dispositivos.

8.4	La protección anti-spam debe filtrar todos los correos electrónicos no deseados y mantener los buzones de correo de los usuarios libres de mensajes no solicitados o indeseados.
8.5	La protección antiphishing debe estar en la capacitad de buscar e identificar enlaces sospechosos de phishing en el cuerpo del mensaje y en el asunto de los mensajes de correo electrónico entrantes, evitado que los usuarios accedan a páginas web de sitios de phishing.
8.6	La protección antispoofing debe identificar y bloquear correos electrónicos fraudulentos que intentan imitar fuentes legítimas. Garantizado una comunicación segura y prevenir ataques de phishing con tecnología de verificación de correos electrónicos.
8.7	Debe escanear los correos electrónicos en busca de caracteres engañosos, incluidos aquellos tomados de distintos alfabetos globales, contra ataques que imitan direcciones de correo legítimas, mejorando la seguridad general del correo electrónico.
8.8	La solución deberá ser capaz de analizar el contenido de Microsoft Exchange Online vía API
8.9	La solución deberá ser capaz de analizar el contenido de Microsoft OneDrive for Business vía API.
8.10	La solución deberá ser capaz de analizar el contenido de Microsoft Sharepoint Online via API
8.11	La solución debe tener cobertura de protección de correo electrónico en nube en Google Workspace. Brindando protección integral a los usuarios de Gmail y Google Drive.
8.12	La solución deberá ser capaz de analizar el contenido de Gmail y Google Drive vía API.
8.13	La solución deberá ser capaz de analizar el contenido de Microsoft Teams via API.
8.14	La solución deberá contar con un servicio integrado de Sandboxing ofrecido por el mismo fabricante.
8.15	Debe detectar el código o comportamiento sospechoso, y evitar mayor actividad de amenazas al colocarlo temporalmente en cuarentena.
8.16	Debe permitir la gestión de correos electrónicos y archivos que se han puesto en cuarentena, con la posibilidad que puedan descargarse los elementos en cuarentena para investigarlos con otras herramientas.
8.17	La solución debe estar en capacidad de enviar archivos adjuntos de correo electrónico sospechosos y archivos de Exchange Online, OneDrive, Grupos del equipo y sitios de SharePoint, para su análisis en nube.
8.18	La solución deberá ser capaz de proporcionar configuraciones de protección basadas en: • Antispam • Anti-Phising • Antimalware • La solución deberá prestar protección inmediata a los usuarios con una política por defecto.
8.19	Debe permitir configuraciones de protección basadas en políticas que puede personalizar en función de sus necesidades y asignar a usuarios y grupos de usuarios, inquilinos o grupos de Team o sitios de SharePoint seleccionados.
8.20	Debe estar en capacidad de configurar la política de forma personalizada y poder asignarse a: • Usuarios: se aplica a usuarios concretos seleccionados manualmente. • Grupos: política que se aplica a todos los miembros del grupo de usuarios. • Inquilinos: política que se aplica a todas las entidades del inquilino. • Grupos de equipos: política que se aplica a grupo de Team. • SharePoint: política que se aplica a un sitio de SharePoint.

8.21	La solución deberá poder proteger de forma inmediata a usuarios que se creen dentro del Tenant de Microsoft.
8.22	Debe proteger la cuenta del usuario, de inquilino de Microsoft que contiene sus usuarios. Los usuarios sin licencia de Microsoft no se mostrarán en la consola de Cloud Office de manera predeterminada. Esto incluye buzones de correo compartidos sin una licencia de Microsoft.
8.23	Debe poder proteger y administrar múltiples inquilinos de Microsoft desde una sola consola Cloud Office. Azure Active Directory (Azure AD) organiza los objetos, como usuarios y aplicaciones, en grupos llamados inquilinos.
8.24	Debe permitir definir políticas sobre los usuarios y aplicaciones de su organización para cumplir con las políticas de seguridad y operativas.
8.25	Desde la consola deberá tener una administración de cuarentena, donde podrá inspeccionar los objetos que están allí y realizar una acción adecuada (descargar, eliminar o liberar).
8.26	La consola debe mostrar datos estadísticos de Exchange Online, OneDrive, grupos del equipo y sitios de SharePoint por correo electrónico, o generar informes únicos para un período elegido.
8.27	La consola debe poder programar informes para que se generen y distribuyan periódicamente a los destinatarios de correo electrónico especificados, el formato de salida del informe será PDF o CSV.
Gestión de vulnerabilidades y parches	
9.1	La plataforma de gestión de vulnerabilidades y parches debe brindar visibilidad de los endpoints, los estados de vulnerabilidades y parches de la organización.
9.2	Debe permitir ejecutar una exploración, que proporcione una descripción de las vulnerabilidades detectadas en los equipos. La exploración debe detectar cualquier herramienta instalada vulnerable y mostrar los riesgos de seguridad.
9.3	El resultado de la exploración debe mostrar informes instantáneos en la consola que permite evaluar y priorizar las vulnerabilidades en función de la gravedad, para así administrar los riesgos de seguridad.
9.4	La gestión de vulnerabilidades y parches debe proporcionar el cumplimiento de normativas como NIS2, FedRAMP, HIPAA, PCI DSS
9.5	Realizar escaneo automatizado sobre del sistema operativo de las endpoints y aplicaciones de terceros, que permita realizar el envío de parches rápidos y automáticos.
9.6	Las políticas de parches personalizables deben brindar flexibilidad y permitir controlar la implementación de parches de seguridad en las endpoints, definiendo franjas horarias específicas para la aplicación de parches.
9.7	La aplicación de parches debe estar respaldada por la protección de contra ransomware y amenazas 0-day.
9.8	Debe analizar gran variedad de aplicaciones y estar en capacidad de detectar más de 35.000 vulnerabilidades y exposiciones comunes (CVE).
9.9	Debe tener opciones de filtrado que permite identificar y centrar rápidamente los problemas críticos de seguridad.
9.10	La solución debe Identificar el software y dispositivos más vulnerables, inventario de parches, incluidos los nombres de los parches, la nueva versión de la aplicación, los números de KB, los CVE, la gravedad/importancia del parche y las aplicaciones afectadas.
9.11	Debe generar Informes de vulnerabilidad del software y dispositivos más expuestos al riesgo.

9.12	Debe estar en la capacidad de configurar las ventanas de mantenimiento y administrar la aplicación de parches según las necesidades específicas: aplicar parches solo a aplicaciones seleccionadas o excluir aplicaciones específicas.
9.13	Debe analizar aplicaciones, como Adobe Acrobat, Mozilla Firefox y Zoom Client, y ser compatible con sistemas operativos Windows, Linux y macOS, el analisis debe aplicar para estaciones de trabajo y servidores.
9.14	Al identificar una vulnerabilidad en el sistema, la información que se muestre en la consola de gestión será: Nombre de la aplicación, Versión de la aplicación, Proveedor, Puntuación de riesgo de 0 a 100, número CVE (vulnerabilidades y exposición comunes), Nombre del equipo, Tipo de sistema operativo.
9.15	La puntuación del riesgo de las vulnerabilidades se clasificará, de acuerdo con los siguientes parámetros. • CVSSv2/CVSSv3 • Popularidad de CVE • Ciclo de vida de CVE • Tasa de riesgo comprometido
9.16	Debe priorizar y filtrar las vulnerabilidades según su puntuación de exposición y gravedad. La puntuación de riesgo mostrada en la consola se indicará de la siguiente manera: • Amarillo (0–40): gravedad media • Rojo (41–100): gravedad crítica
9.17	Se debe allegar con la oferta, una certificación del fabricante o mayorista, en donde consta que el partner está certificado, cuenta con la experiencia para manejar el producto, y tiene todo el respaldo del fabricante para el afinamiento y soporte de la solución.
Instalación y configuración	
10	La herramienta de seguridad debe entregarse instalado y configurado en la entidad (usuarios finales), sin costo adicional para el INPEC. Incluir capacitación para funcionarios de la entidad.
Vigencia	
11	La herramienta de seguridad debe tener una vigencia de 12 meses a nombre del Instituto Nacional penitenciario y carcelario - INPEC. Durante la vigencia se debe actualizar la herramienta de seguridad de acuerdo a las versiones estables emitidas por el fabricante.
Certificación	
12	El proponente debe acreditar mediante certificación expedida por el Fabricante que es Distribuidor Autorizado de la herramienta ofrecida y que está en capacidad técnica para atender los requerimientos relacionados con el Soporte Técnico.
Personal mínimo requerido para la ejecución del proyecto	
13	Generalidades: El proponente debe acreditar que cuenta con el siguiente personal mínimo para la conformación del equipo de trabajo, entregando los respetivos soportes con su oferta, hoja de vida y documentos soporte de las personas que harán parte del equipo de trabajo, con el fin de verificar el cumplimiento de lo requerido:
13.1	Un (1) Gerente de Proyectos: Profesional en Ingeniería de Sistemas / Ingeniería Informática / Ingeniería electrónica / Ingeniería de Software / Ingeniería de Telecomunicaciones o afines. Anexar copia de la tarjeta profesional y certificado de antecedentes disciplinarios. Con postgrado: Especialización y/o Maestría en Gerencia de Proyectos o Seguridad de

	Redes o Seguridad de la Información o Telemática. Debe Contar como mínimo con dos de las siguientes certificaciones vigentes: • PMP • ISO 27001 • ITIL v4 • Scrum Master Experiencia general: Contar con mínimo seis (6) años de experiencia general contados a partir de la expedición de la tarjeta profesional. Experiencia Específica: Experiencia mínima de cinco (3) años ejerciendo cargos relacionados con funciones de gerencia de proyectos de tecnología y/o gerencia de proyectos de Ciberseguridad.
13.2	Un (1) Especialista en Implementación de la herramienta de seguridad para usuario final: Profesional en Ingeniería electrónica / Ingeniería telemática / Ingeniería de sistemas / Ingeniería de telecomunicaciones o afines. Anexar copia de la tarjeta profesional y certificado de antecedentes disciplinarios. Debe anexar la Certificación del fabricante de la solución ofertada, que lo certifica como profesional idóneo para la implementación de la herramienta de seguridad para usuario final ofertada. Esta certificación debe haber sido emitida con una antigüedad no mayor a treinta días a la fecha de cierre del presente proceso. Experiencia General: mínimo cinco (5) años de experiencia general contados a partir de la expedición de la tarjeta profesional. Experiencia Específica: mínimo de tres (3) años en al menos un (1) proyecto de solución de seguridad endpoint con características similares al objeto del presente proceso, ejerciendo cargos relacionados con la configuración, implementación y administración de soluciones de seguridad endpoint.

Nota No 1: Las cantidades mencionadas pueden aumentar según el resultado de la subasta, hasta agotar los recursos disponibles, por lo cual, el presente proceso de selección será adjudicado por el valor total del presupuesto oficial, aumentando si a ello hubiere lugar las cantidades a implementar de la herramienta de seguridad, hasta completar el valor del presupuesto oficial, teniendo en cuenta el valor unitario ofertado.

Nota No. 2: Las especificaciones técnicas descritas son de carácter obligatorio. No obstante, en caso de que el oferente omita adjuntar soporte documental que demuestre el cumplimiento de alguna de estas características, dicha omisión podrá ser objeto de subsanación, de acuerdo a los términos establecidos en el artículo 5 de la ley 1882 de 2018.

2.3 IDENTIFICACIÓN DEL CONTRATO A CELEBRAR

Contrato de Compraventa.

2.4 PLAZO DE EJECUCIÓN

El plazo de ejecución y entrega total de la herramienta de seguridad para usuario final debidamente instalada y en perfecto funcionamiento, previa aprobación del supervisor del contrato, será hasta el 15 de diciembre de 2025, previa aprobación de la Garantía de Cumplimiento de las Obligaciones Contractuales, por parte de la Subdirección de Gestión Contractual y Registro Presupuestal.

DOMICILIO CONTRACTUAL

Para todos los efectos legales, el domicilio contractual se fija en la ciudad de Bogotá. D.C. calle 26 # 27-48, edificio del Instituto Nacional Penitenciario y Carcelario – INPEC.

FORMA DE PAGO

El Instituto Nacional Penitenciario y Carcelario, pagará al CONTRATISTA el valor del contrato, con cargo al presupuesto del INPEC, en pesos colombianos así:

El INPEC, pagará el 100% del contrato a la entrega de la herramienta de seguridad instalado, configurado e integrado con las plataformas existentes en la entidad, previa certificación del supervisor y la presentación de la factura electrónica por parte del contratista, quien deberá acreditar el pago de los aportes parafiscales relativos al sistema de seguridad social integral, así como los aportes al SENA, ICBF y Caja de Compensación Familiar, si hubiere lugar a ello.

La factura electrónica emitida por la empresa en cumplimiento al Decreto 2242 de 2015, Resoluciones y sus modificaciones, será cancelada por el INPEC dentro de los treinta (30) días siguientes a la fecha de radicación de la misma con sus soportes, en concordancia con lo establecido en el articulado 615 y 617 del Estatuto Tributario, previa certificación del supervisor del contrato, donde conste el cumplimiento a satisfacción del objeto contractual, antecedente revisión de la unidad ejecutora que tiene a su cargo la recepción, verificación y aprobación en la Dirección de Gestión Corporativa, previa disponibilidad del PAC.

Si la factura no ha sido correctamente elaborada o no se acompañan de los documentos requeridos para pago, el término se contará desde la fecha en que se presente en debida forma o se aporte el último de los documentos.

PRESUPUESTO ASIGNADO

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.

2.5 LUGAR DE PRESTACION DEL SERVICIO

La instalación y puesta en funcionamiento se realizará así:

SEDE CENTRAL INPEC
Calle 26 No. 27-48 – Edificio Instituto Nacional Penitenciario y Carcelario – INPEC
Bogotá – Cundinamarca.

Sedes INPEC previo disposición del supervisor del contrato

2.6 OBLIGACIONES DEL CONTRATISTA

Además de los deberes señalados en el artículo 5 de la Ley 80 de 1993, el CONTRATISTA contrae las siguientes obligaciones:

1. Entregar, instalar y dejar en correcto funcionamiento la herramienta de seguridad para usuario final, de conformidad con las especificaciones técnicas mínimas establecidas en el estudio previo, pliego de condiciones y demás documentos contractuales.

2. Para la entrega, implementación y puesta en funcionamiento, el contratista realizará pruebas de afinamiento en coordinación con el supervisor del contrato, cuyos resultados deberán dar cumplimiento a lo requerido en la ficha técnica para la suscripción del acta de recibo a satisfacción.

3. Ejecutar el contrato dentro del término establecido y realizar las actividades en los plazos definidos en el cronograma aprobado por el supervisor del contrato.

4. Coordinar con el supervisor del contrato cualquier programación de actividades en fines de semana, horario nocturno o festivos, sin que esto genere costos adicionales para el INPEC.

5. Resolver oportunamente los requerimientos de aclaración de información y los cambios que se presenten durante la ejecución del contrato según las directrices del supervisor.

6. Cumplir con los requisitos de perfeccionamiento, ejecución y legalización del contrato, así como con las obligaciones establecidas en la oferta presentada.

7. No acceder a peticiones o amenazas ilegales de terceros y, en caso de presentarse, informar de inmediato a la Subdirección de Gestión Contractual y a las autoridades competentes.

8. Garantizar que el personal asignado por el contratista esté vinculado y afiliado al sistema de seguridad social integral conforme a la normatividad vigente.

9. Presentar certificación de cumplimiento de pagos de seguridad social, salud, pensiones y aportes parafiscales (SENA, ICBF y caja de compensación), de acuerdo con lo dispuesto en la ley.

10. Restituir al INPEC cualquier elemento que le haya sido entregado en comodato o puesto a disposición durante la ejecución contractual, cuando se lo requiera o al finalizar el contrato.

11. Entregar al INPEC la relación del personal asignado a la ejecución contractual para efectos de validación y autorización de ingreso a las instalaciones. En caso de incumplir requisitos, el contratista deberá reemplazarlo por personal idóneo aprobado por el INPEC.

12. Proveer los equipos, herramientas, insumos y conectividad que resulten necesarios para la correcta instalación, despliegue y configuración de la herramienta de seguridad para usuario final, sin generar costos adicionales al INPEC.

13. Cumplir estrictamente las especificaciones técnicas de la herramienta de seguridad para usuario final, incluyendo funcionalidades, características de gestión y niveles de protección establecidos en el pliego de condiciones.

14. Mantener indemne al INPEC frente a daños, perjuicios o reclamaciones derivados del incumplimiento contractual, o de incidentes ocasionados por la ejecución del contrato.

15. Informar oportunamente al supervisor cualquier interrupción temporal en la instalación o puesta en funcionamiento de la herramienta de seguridad para usuarios finales, proponiendo un plan de acción de continuidad.

16. Cumplir con todas las normas reglamentarias de seguridad y salud en el trabajo, medicina preventiva e higiene, aplicables durante la ejecución contractual en instalaciones del INPEC.

17. Corregir sin costo adicional para el INPEC cualquier falla de funcionamiento de la herramienta de seguridad para usuario final detectada durante la ejecución contractual o dentro del periodo de garantía, de conformidad con la Ley 1480 de 2011 y demás normas aplicables.

18. Disponer del personal técnico idóneo y certificado por el fabricante para realizar soporte técnico de la implementación y funcionamiento general de la herramienta de seguridad para usuario final.

19. Implementar medidas de seguridad industrial y, en caso de actividades presenciales, realizar la debida demarcación de áreas de trabajo en coordinación con el supervisor del contrato.

20. Prestar los servicios de soporte correctivo y preventivo de la herramienta de seguridad para usuario final durante la vigencia de la garantía, gestionando actualizaciones y parches directamente con el fabricante.

21. Asumir los costos adicionales de personal o recursos necesarios para garantizar el cumplimiento de los plazos contractuales establecidos.

22. Dirigir personalmente y bajo su responsabilidad la ejecución del contrato, garantizando autonomía técnica y administrativa.

23. Mantener disponible el personal exigido en las especificaciones técnicas durante toda la ejecución contractual. En caso de reemplazo, deberá acreditarse un perfil igual o superior al inicialmente exigido, con aprobación previa del supervisor.

24. Reemplazar, previa autorización del supervisor, cualquier miembro del equipo de trabajo que no cumpla satisfactoriamente con las funciones encomendadas.

25. Ejecutar el contrato con plena autonomía técnica y administrativa, sin que se genere vínculo laboral alguno entre el INPEC y el personal del contratista.

26. Retirar a su cuenta y riesgo los elementos, insumos o residuos generados durante la instalación o despliegue de la solución.

27. Entregar un cronograma detallado de actividades que incluya tiempos de instalación, despliegue, configuración y puesta en funcionamiento de la solución, previa aprobación del supervisor.

28. Guardar estricta confidencialidad sobre toda información del INPEC a la que tenga acceso durante la ejecución contractual, respondiendo civil y penalmente por su divulgación o uso indebido.

29. Firmar acuerdos de confidencialidad y compromisos de seguridad de la información para todo el personal que tenga acceso remoto o presencial a los sistemas o instalaciones del INPEC en desarrollo del contrato.

30. Cumplir con las demás obligaciones contenidas en las especificaciones técnicas, el estudio previo, el pliego de condiciones y los documentos derivados del proceso de selección contractual.

OBLIGACIONES DEL INPEC

1. Vigilar la debida y oportuna ejecución del contrato y el cumplimiento de todas las obligaciones contractuales a través del Supervisor del Contrato.

2. Expedir la certificación del recibo a satisfacción de la solución, en cumplimiento del objeto contractual pactado, para efectos del pago, de conformidad con lo señalado en el contrato.

3. Realizar los pagos de forma oportuna, siempre y cuando el CONTRATISTA presente todos los documentos, requisitos y soportes establecidos para tal efecto.

4. Analizar y responder los requerimientos que formule el contratista con ocasión del Contrato.

5. Comunicar por escrito al CONTRATISTA cualquier reclamación por deficiencia en los bienes a adquirir.

6. Todas las demás que permitan el cabal cumplimiento de las condiciones previstas en los Estudios Previos, Pliego de Condiciones y el Contrato.

2.7 SUPERVISIÓN DEL CONTRATO

La supervisión del contrato, estará a cargo del Coordinador del Grupo Administración de las Tecnologías de Información o quien haga sus veces, o quien el ordenador del gasto designe por escrito.

Quienes verificarán la ejecución idónea y el cumplimiento del objeto del contrato de acuerdo con las funciones asignadas para el efecto en el manual de contratación y en cumplimiento a lo dispuesto en la ley 1474 de 2011, artículos 83 y 84 en cuanto al seguimiento técnico, administrativo, financiero, contable y jurídico del objeto contractual.

3. MODALIDAD DE SELECCIÓN DEL CONTRATISTA Y SU JUSTIFICACIÓN, INCLUYENDO LOS FUNDAMENTOS JURÍDICOS

De acuerdo al plan de Compras de la presente vigencia, y conforme al concepto jurídico bajo radicado No. 2025IE0156291 de fecha 04 de agosto de 2025, emitido por la Subdirección de Gestión Contractual, al respecto:

MODALIDAD DE SELECCIÓN: La modalidad de selección que se debe tener en cuenta para la CONTRATACIÓN es la de SELECCIÓN ABREVIADA, con el procedimiento de SUBASTA INVERSA, reglamentada por el numeral 2, artículo 2, de la Ley 1150 del 2007, que a la letra señala:

*"2. **Selección abreviada**. La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que, por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio, puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.*

El Gobierno Nacional reglamentará la materia.

Serán causales de selección abreviada las siguientes:

a) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellas que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos.

*Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, **hacer uso de procedimientos de subasta inversa** o de instrumentos de compra por catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos;" Negrilla fuera de texto*

De igual forma se debe tener en cuenta lo establecido en el Artículo 2.2.1.2.1.2.1 al 2.2.1.2.1.2.4 del Decreto 1082 de 2015, que establece el procedimiento de la Subasta Inversa.

El Plan Anual de Adquisiciones Vigencia Fiscal 2025 del INPEC, figura:

No. AGRUPACIÓN	BS ITEM	DESCRIPCIÓN	Apropiación Presupuestal 2025	Dependencia que requiere la necesidad	Dependencia o Grupo Responsable de estructurar proceso	Modalidad Contractual
35	519	Adquisición de herramienta de seguridad de usuario final	$ 300.000.000	Oficina de Sistemas de Información	Oficina de Sistemas de Información	SELECCIÓN ABREVIADA POR SUBASTA INVERSA

Así mismo, el presente concepto se tendrá en cuenta, siempre que exista el respectivo CDP para la vigencia 2025. No obstante, se recuerda que esta procede conforme a la aprobación por parte del Director General del plan anual de adquisición para la vigencia 2025.

3.1. MARGEN MINIMO DE MEJORA DE OFERTAS

Los oferentes harán su lance utilizando los sobres y formularios suministrados o la plataforma de SECOP II para la subasta electrónica. La entidad establece como margen mínimo de diferencia entre lances de precio el TRES POR CIENTO (3%) POR GRUPO, en consecuencia, solo serán válidos los lances que observando el margen mínimo mejoren el precio de arranque o el menor precio de la ronda anterior según el caso.

4. VALOR ESTIMADO DEL PROCESO DE CONTRATACIÓN.

Debido a la naturaleza y las condiciones de la solución que se requiere, para el presente proceso contractual pueden participar tanto las personas Naturales o Jurídicas, que cumplan cada una 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. Con el fin de realizar el análisis de la oferta, se solicitó a diferentes Personas Naturales o Jurídicas que coticen lo establecido en la ficha técnica conforme al objeto del contrato, procediendo a remitir las especificaciones técnicas vía correo electrónico institucional 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	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

de las cuales se recibieron tres (03) cotizaciones de acuerdo a la ficha técnica establecida para la solución con exclusión de IVA, de las empresas que se enuncian a continuación:

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 por unidad. Con base en dicho cálculo, se determina el número de licencias 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.

4. REQUISITOS HABILITANTES PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

El procedimiento de selección del contratista está sometido a los principios de transparencia, economía y responsabilidad y de conformidad con los postulados que rigen la función pública y las normas que regulan la conducta de los servidores públicos, teniendo en cuenta la modalidad de selección objetiva en igualdad de derechos y oportunidades de los que se deriva la obligación de someter a todos los oferentes a las mismas condiciones definidas en la ley y en el pliego de condiciones.

La ley 1474 de 2011, articulo 88, que modifica el numeral 2 del artículo 5 de la Ley 1150 DE 2007 estipula que: *"La oferta más favorable será aquella que, teniendo en cuenta los factores técnicos y económicos de escogencia y la ponderación precisa y detallada de los mismos, contenida en los pliegos de condiciones o sus equivalentes, resulte ser la más ventajosa para la entidad, sin que la favorabilidad la*

constituya factores diferentes a los contenidos en dichos documentos"

Así mismo el numeral 3 del artículo 5 de la ley 1150 de 2007 establece que *"para las contrataciones cuyo objeto sea la adquisición o suministros de bienes y servicios de características técnicas uniformes y común utilización, las entidades estatales incluirán como único factor de evaluación el menor precio ofrecido".*

4.1 Requisitos De Orden Financiero

En atención al oficio con radicado 2025IE0160471 de fecha 11 de agosto de 2025, suscrito por la Coordinadora del Grupo Contable se emite concepto financiero para el presente proceso contractual, de igual manera mediante oficio con GESDOC 2025IE0164908 de fecha 15 de agosto de 2025 suscrito por la Coordinadora Grupo Contable, se realiza alcance al concepto financiero emitido, el cual se debe tener en cuenta para este proceso de contratación, rubro: A-02-01-01-006-002, recurso 10, BSITEM 519, valor $300.000.000, donde se define que la capacidad financiera será la que se describe a continuación:

Capacidad Financiera

El Instituto Nacional Penitenciario y Carcelario – INPEC, efectúo un análisis para establecer los indicadores financieros para verificar la capacidad financiera de acuerdo con el Decreto 1082 de 2015.

De conformidad con lo anterior, el Instituto analizó los estándares correspondientes al sector económico relacionado con la actividad del sector económico a contratar. En el entendido que el análisis financiero debe hacerse en forma integral y con base en el propósito para la cual se está realizando; la Entidad considera que una capacidad financiera razonable minimiza el riesgo en el cumplimiento de la ejecución del contrato producto del proceso y que garantiza pluralidad de oferentes al proceso. La Capacidad financiera debe ser adecuada y proporcional a la naturaleza y el valor del contrato.

Los Estados Financieros a tener en cuenta para verificar la capacidad financiera del presente proceso, serán con fecha de corte a 31 de diciembre de 2024, los cuales serán verificados en el RUP vigente y en firme a la fecha de cierre del proceso.

La Capacidad Financiera del presente proceso, se realizará de acuerdo con lo establecido en el Manual de Requisitos Habilitantes expedido por Colombia Compra Eficiente y se verificará teniendo en cuenta la información contenida en el Registro Único de Proponentes– RUP actualizada a 31 de diciembre de 2024. Este certificado deberá haber sido expedido máximo dentro de los treinta (30) días anteriores a la fecha de cierre del proceso de selección.

Los proponentes a presentarse sean personas jurídicas o personas naturales deben tener como mínimo un (1) año de constituida la entidad.

Este aspecto no otorgará puntaje, pero habilitará o deshabilitará la propuesta. Se evaluará con **CUMPLE o NO CUMPLE**.

INDICADORES FINANCIEROS Y ORGANIZACIONALES DE PROPONENTES EXTRANJEROS

Para este aspecto *la "Guía para la participación de Proveedores Extranjeros en Procesos de Contratación"* emitida por Colombia Compra Eficiente establece:

"Los proveedores extranjeros deben presentar los estados financieros del año inmediatamente anterior, debidamente auditados en las condiciones definidas en los pliegos de condiciones, que deben contener los elementos para hacer la conversión de los estados financieros que

fueron expedidos en moneda extranjera. Cuando, de acuerdo con las normas aplicables, los proveedores extranjeros "aprueben sus estados financieros auditados con corte a 31 de diciembre en una fecha posterior al quinto día hábil del mes de abril, pueden presentar sus estados financieros a 31 de diciembre suscritos por el representante legal junto con un pre informe de auditoría en el cual el auditor o el revisor fiscal certifique que: (a) la información financiera presentada a la Entidad Estatal es la entregada al auditor o revisor fiscal para cumplir su función de auditoría; y (b) el proponente en forma regular y para ejercicios contables anteriores ha adoptado normas y principios de contabilidad generalmente aceptados para preparar su información y estados financieros. (...). Esta información debe ser actualizada llegada la fecha máxima de actualización de acuerdo con la legislación del país de origen".

INDICADORES FINANCIEROS

Las definiciones para los indicadores de Capacidad Financiera y Organizacional son las siguientes:

Índice de Liquidez. Activo Corriente / Pasivo Corriente, el cual determina la capacidad que tiene un proponente para cumplir con sus obligaciones de corto plazo. A mayor índice de liquidez, menor es la probabilidad de que el proponente incumpla sus obligaciones de corto plazo.

Índice de Endeudamiento. Pasivo Total / Activo Total, el cual determina el grado de endeudamiento en la estructura de financiación (pasivos y patrimonio) del proponente. A mayor índice de endeudamiento, mayor es la probabilidad del proponente de no poder cumplir con sus pasivos.

Razón de Cobertura de Intereses. Utilidad Operacional / Gastos de Intereses, el cual refleja la capacidad del proponente de cumplir con sus obligaciones financieras. A mayor cobertura de intereses, menor es la probabilidad de que el proponente incumpla sus obligaciones financieras.

Rentabilidad del Activo. Utilidad Operacional / Activo Total, el cual determina la rentabilidad de los activos del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el activo. A mayor rentabilidad sobre activos, mayor es la rentabilidad del negocio y mejor la capacidad organizacional del proponente.

Rentabilidad del Patrimonio. Utilidad Operacional/ Patrimonio, el cual determina la rentabilidad del patrimonio del proponente, es decir, la capacidad de generación de utilidad operacional por cada peso invertido en el patrimonio. A mayor rentabilidad sobre el patrimonio, mayor es la rentabilidad de los accionistas y mejor la capacidad organizacional del proponente.

INDICADORES FINANCIEROS

CAPACIDAD FINANCIERA	CAPACIDAD ORGANIZACIONAL	MARGEN REQUERIDO
LIQUIDEZ		MINIMO 1.2
ENDEUDAMIENTO		MAXIMO 50%
RAZON COBERTURA DE INTERESES		MAYOR O IGUAL A 1.3
	RENTABILIDAD DEL ACTIVO	MAYOR O IGUAL AL 1.3%
	RENTABILIDAD DEL PATRIMONIO	MAYOR O IGUAL AL 1.3%

Los proponentes que no tengan gastos de intereses y cuya utilidad operacional sea positiva, quedan habilitados respecto del indicador de cobertura de intereses.

Los proponentes que presenten una utilidad operativo negativa o igual a cero (0), **NO** cumplirán con el indicador solicitado.

Los proponentes que presenten una utilidad operativa negativa **NO** cumplirán con los indicadores solicitados al mostrar rendimientos negativos.

CÁLCULO DE ÍNDICES FINANCIEROS

A. INDICE DE LIQUIDEZ: (ACTIVO ORRIENTE/PASIVO CORRIENTE)
B. NIVEL DE ENDEUDAMIENTO TOTAL: (PASIVO TOTAL/ACTIVO TOTAL X 100%)
C. RAZON COBERTURA DE INTERESES: (UTILIDAD OPERACIONAL/GASTOS DE INTERESES)
D. RENTABILIDAD DEL ACTIVO: (UTILIDAD OPERACIONAL/ ACTIVO TOTAL)
E. RENTABILIDAD DEL PATRIMONIO: (UTILIDAD OPERACIONAL / PATRIMONIO)

En caso de **UNIONES TEMPORALES o CONSORCIOS**, los indicadores, se obtendrán de la sumatoria de las cifras registradas en cada uno de los balances de los miembros que la conforman, aplicando las anteriores formulas. Los indicadores de rentabilidad del activo y rentabilidad del Patrimonio, cada integrante deberá cumplir con el mínimo requerido.

Indicador	Formula Oferente Individual	Formula Oferente Plural
Índice de Liquidez	Activo Corriente/Pasivo Corriente	L = ((∑ (ACn x %n) ÷∑ (PCn x %n))
Índice de Endeudamiento	(Pasivo Total/ Activo Total) x 100	E = ((∑ PTn x %n) ÷∑(ATn x %n)) x 100
Razón Cobertura de Intereses	Utilidad Operacional/ Gastos Intereses	CI = ((∑ (UOn x %n) ÷∑ (GI n x %n))
Rentabilidad del Activo	(Utilidad Operacional/ Activo Total) x 100	RA = ((∑ (UOn x %n) ÷ ∑ (ATn x %n)) x 100
Rentabilidad del Patrimonio	(Utilidad Operacional/ Patrimonio) x 100	RP = ((∑ (UOn x %n) ÷ ∑ (Pn x %n)) x 100

Dónde:

ACn = Activo Corriente de cada integrante de consorcio o unión temporal.
PCn = Pasivo Corriente de cada integrante de consorcio o unión temporal.
PTn = Pasivo Total de cada integrante de consorcio o unión temporal.
ATn = Activo Total de cada integrante de consorcio o unión temporal.
UOn = Utilidad Operacional de cada integrante de consorcio o unión temporal.
GI n = Gastos de intereses de cada integrante de consorcio o unión temporal.
%n = Porcentaje de Participación de cada integrante de consorcio o unión temporal.
Pn = Patrimonio de cada integrante de consorcio o unión temporal.

Nota 1: Para el caso de consorcios o uniones temporales o promesa de sociedad futura, se tomará el promedio ponderado de cada uno de los integrantes, de acuerdo con su porcentaje

de participación, así como lo señala la fórmula para oferente plural en la tabla anterior.

Nota 2: Para los proponentes que no presenten gastos de intereses y que la utilidad operacional sea positiva, quedan habilitados respecto al indicador de cobertura de intereses.

Nota 3: Para calcular el indicador de cobertura de intereses, si la totalidad de los integrantes del consorcio o unión temporal presenta como gastos de intereses un valor de cero (0), no se podrá calcular dicho indicador, en este caso el oferente plural **CUMPLE**. Si el resultado de este indicador es negativo, el proponente plural **NO CUMPLE**.

Para la evaluación de proponentes singulares, en el indicador de razón de cobertura de intereses, los oferentes cuyos gastos de intereses sean cero (0), no podrán calcular dicho indicador, en este caso el oferente CUMPLE. Si su utilidad operacional es negativa, el proponente singular NO CUMPLE.

Nota 4: En el caso que la Utilidad operacional sea negativa para oferente individual, o que el resultado del indicador sea negativo para oferentes plurales, se calificará como NO CUMPLE.

En lo correspondiente a los impuestos, se comunica lo siguiente:

PROCESO	IVA	RETENCIONES
"ADQUISICION DE HERRAMIENTAS DE SEGURIDAD USUARIO FINAL". BSITEM 519	EXCLUIDO DE IVA ARTICULO 476 ET Numeral 20	RETENCIÓN EN LA FUENTE RENTA POR COMPRAS. RETENCIÓN EN LA FUENTE ICA POR COMPRAS.

Durante la ejecución del contrato el prestador del servicio debe asumir las demás cargas tributarias de carácter legal del orden nacional, departamental y municipal a que haya a lugar.

5. EXPERIENCIA DEL PROPONENTE

Experiencia contenida en el Registro Único de Proponentes

Para efectos de verificación de este requisito, deberán acreditar en el Registro Único de Proponentes experiencia relacionada con el objeto del presente proceso. Experiencia que será verificada en máximo tres (3) certificaciones de contratos ejecutados y finalizados con entidades públicas y/o privadas antes del cierre de la presente contratación, en el entendido que si se presentan tres contratos, cada uno de ellos debe tener registrado mínimo un código UNSPSC, si presenta un contrato este debe tener registrado mínimo los tres códigos UNSPSC requeridos; que sumadas sus cuantías sean igual o superior al presupuesto oficial estimado para la presente contratación expresada en salarios mínimos legales mensuales vigentes al momento de la ejecución del contrato, es decir de 210,72 SMMLV

Si la propuesta es presentada por un Consorcio o por una Unión Temporal o por cualquier otra forma de asociación, la experiencia podrá ser acreditada por cualquiera de sus integrantes. El integrante que acredite la mayor experiencia, deberá tener por lo menos el 50% de participación en la figura asociativa.

Una empresa apta para cumplir el bien en las condiciones exigidas, debe presentar una

experiencia en el RUP igual o superior al valor del contrato.

El proponente debe demostrar que los contratos aportados están registrados hasta el tercer nivel (clase) como mínimo tres códigos de los siguientes por ítem:

CLASIFICACIÓN	SEGMENTO	FAMILIA	CLASE
43222500	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de seguridad de red
43233200	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de Seguridad y Protección
43233700	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de administración de sistemas
80101600	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	Servicios de asesoría de gestión	Gerencia de Proyectos
81111500	Servicios basados en Ingeniería, Investigación y tecnología	Servicios informáticos	Ingeniería de software o hardware

Para acreditar la experiencia, deberá allegar debidamente diligenciado el Anexo "Experiencia" el cual debe ser allegado junto con la propuesta en el cual se relacionen los contratos que pretende hacer valer dentro del proceso.

VALOR ESTIMADO DEL CONTRATO	VALOR ESTIMADO DEL CONTRATO EN SMMLV
$ 299.962.131	**210,72**

La experiencia podrá ser continua o discontinua.

El proponente deberá convertir los valores de los contratos relacionados en el anexo correspondiente, a Salarios Mínimos Mensuales Legales Vigentes, dividiendo el valor del contrato por el Salario Mínimo Legal Mensual Vigente a la fecha de suscripción del mismo, de acuerdo con la siguiente tabla ilustrativa o la conversión del valor en SMMLV del año a que corresponda:

PERÍODO	SMLMV
Enero 1 de 2018 a Diciembre 31 de 2018	781.242,00
Enero 1 de 2019 a Diciembre 31 de 2019	828.116.00
Enero 1 de 2020 a Diciembre 31 de 2020	877.803,00
Enero 1 de 2021 a Diciembre 31 de 2021	908.526,00
Enero 1 de 2022 a Diciembre 31 de 2022	1.000.000,00
Enero 1 de 2023 a Diciembre 31 de 2023	1.160.000,00

Enero 1 de 2024 a Diciembre 31 de 2024	1.300.000,00
Enero 1 de 2025 hasta la fecha	1.423.500,00

Este aspecto no da lugar a puntaje, sin embargo, será objeto de verificación como requisito habilitante. Las certificaciones de los contratistas que respalden la experiencia, deben tener como mínimo la siguiente información:

a) Nombre o razón social del contratante
b) Nombre o razón social del contratista
c) Objeto claramente definido
d) Numero de contrato
e) Fecha de iniciación del contrato
f) Fecha de terminación del contrato
g) Valor del contrato (Valor del contrato principal más adiciones)
h) Firma y nombre del Representante del contratante o de la persona autorizada para expedirla.
i) Porcentaje de participación de cada uno de los integrantes del Consorcio o de la Unión Temporal, cuando la experiencia que se pretenda certificar corresponda a un contrato ejecutado en alguna de esas modalidades de asociación; en este evento solo se tendrá en cuenta la participación del oferente.
j) fecha, firma y cargo del funcionario que expide la certificación.
k) constancia de recibo o satisfacción por el contratante o que de la certificación se infiera el cumplimiento o ejecución del contrato.

La entidad no acepta que cada renovación automática de un contrato se cuente como un nuevo contrato, en razón que el contrato es uno solo y el hecho de prorrogarlo o adicionarlo no significa que se celebre un nuevo negocio contractual. De esta forma su cumplimiento se verifica desde el inicio hasta la culminación del mismo, entendiendo que ha finalizado cuando ha terminado su última renovación.
En los contratos certificados y que fueron ejecutados como miembro de consorcio, en unión temporal, sociedad de objeto único, empresa unipersonal o sociedades en general, deberá indicarse el porcentaje de participación de cada uno de ellos en dicho contrato, valor que debe discriminarse en pesos colombianos y será el que se aplique al proponente para verificar la experiencia teniendo en cuenta lo señalado en este numeral.

En cada certificación, se debe señalar que el contratista cumplió satisfactoriamente.

Requisitos

Las certificaciones sobre experiencia, seriedad y cumplimiento del proponente, deben ser expedidas únicamente por el contratante y suscritas por las personas competentes o autorizadas para ello.

En los casos en que el contrato o los contratos hayan sido celebrados en consorcio, unión temporal o bajo cualquier otra forma de participación conjunta, será tenido en cuenta el valor de acuerdo al porcentaje de participación

En caso de presentarse certificaciones por contratos adicionales, estos se evaluarán en conjunto con el contrato principal al que están adicionando. Para el efecto, la certificación deberá contener como mínimo el valor del contrato adicional y la fecha de su celebración.

En caso de hallarse inconsistencias entre la información registrada en el RUP y los datos señalados en las constancias o certificaciones, se tendrá solamente en cuenta la información registrada en el RUP.

En el caso que la certificación no contenga todos los datos anteriormente mencionados se podrá complementar, con el acta de Liquidación del Contrato, en la que aparezcan los datos faltantes, siempre y cuando en la misma conste que el contrato se cumplió a satisfacción

Se aceptan certificaciones dirigidas a otra entidad, siempre y cuando del contenido de éstas, se pueda certificar el cumplimiento de los requisitos que se exigen.

El INPEC se reserva el derecho de verificar la autenticidad de las certificaciones aportadas o de solicitar los respectivos contratos o documentos que la soporten.

En los casos en que se haya suscrito más de un (1) contrato con una misma Entidad, se deben relacionar por separado los datos de cada contrato Estas certificaciones son solo requisito mínimo o habilitante, no otorgarán puntaje Tratándose de consorcios o unión temporal, este requisito puede ser cumplido por cualquiera de sus integrantes.

Para efectos de la verificación de la experiencia, el proponente deberá diligenciar la información solicitada en el anexo correspondiente del pliego de condiciones.

LAS COPIAS DE CONTRATOS, ACTAS DE LIQUIDACIÓN, RELACIÓN DE CONTRATOS, REFERENCIAS COMERCIALES, ENTRE OTROS, SÓLO SE ACEPTARÁN COMO DOCUMENTOS ACLARATORIOS DE LAS CERTIFICACIONES DE EXPERIENCIA Y CUMPLIMIENTO PRESENTADAS Y NO COMO DOCUMENTOS PARA ACREDITAR LA INFORMACIÓN EXIGIDA EN LAS MISMAS.

Certificados de Distribuidor Autorizado y Garantías

El proponente deberá presentar con su propuesta, las certificaciones del fabricante de los bienes Ofertados que se mencionan en la ficha técnica, en donde lo acredite como distribuidor autorizado de la marca.

De igual forma el proponente deberá presentar con su propuesta que cuenta con disponibilidad inmediata del personal presentado, para ello deberá adjuntar la hoja de vida y la autorización para presentarla en el presente proceso, las cuales serán evaluadas dentro del proceso de selección.

6. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

El procedimiento de selección del contratista está sometido a los principios de transparencia, economía y responsabilidad y de conformidad con los postulados que rigen la función pública y las normas que regulan la conducta de los servidores públicos, teniendo en cuenta la modalidad de selección objetiva en igualdad de derechos y oportunidades de los que se deriva la obligación de someter a todos los oferentes a las mismas condiciones definidas en la ley y en el pliego de condiciones.

La ley 1474 de 2011, articulo 88, que modifica el numeral 2 del artículo 5 de la Ley 1150 DE

2007 estipula que: "La oferta más favorable será aquella que, teniendo en cuenta los factores técnicos y económicos de escogencia y la ponderación precisa y detallada de los mismos, contenida en los pliegos de condiciones o sus equivalentes, resulte ser la más ventajosa para la entidad, sin que la favorabilidad la constituya factores diferentes a los contenidos en dichos documentos"

Así mismo el numeral 3 del artículo 5 de la ley 1150 de 2007 establece que "para las contrataciones cuyo objeto sea la adquisición o suministros de bienes y servicios de características técnicas uniformes y común utilización, las entidades estatales incluirán como único factor de evaluación el menor precio ofrecido".

Así mismo el artículo 2.2.1.2.1.2.4 del Decreto 1082 de 2015 establece que en las subastas inversas para la adquisición de bienes y servicios de características técnicas uniformes y de común utilización, la entidad estatal debe adjudicar el contrato al oferente que haya presentado el lance más bajo.

CONDICIONES MINIMAS EXCLUYENTES

Los proponentes deben acreditar el cumplimiento de las especificaciones requeridas, y condiciones especiales mínimas definidas en la ficha técnica. Para ello acreditara su cumplimiento conforme se señale en el pliego de condiciones.

7. ANALISIS DEL RIESGO Y LA FORMA DE MITIGARLO

El análisis de los riesgos aporta una información indispensable para adoptar las medidas apropiadas para el tratamiento de los riesgos en sus vertientes estratégicas, técnicas y económicas. Al actuar frente a los riesgos se parte de una información obtenida de experiencias pasadas, a veces de dudosa validez, por lo que pueden no ser apropiadas para buscar la protección futura. A menudo, al carecer de experiencias con respaldo estadístico, se hace necesario acudir a hipótesis "Posibilistas", que no tienen una base científica (no se pueden conseguir por falta de medios), pero que se convierten en los únicos elementos de valoración para la toma de decisiones y, por tanto, de gran valor práctico.

7.1 MATRIZ DE RIESGO

De acuerdo a lo establecido por el artículo 4º de la Ley 1150 de 2007 numeral 6 del artículo 2.2.1.1.2.1.1 y 2.2.1.1.1.6.3 del Decreto 1082 de 2015, Documento CONPES 3714 de 2011 y el Manual para la Identificación y Cobertura del Riesgo de Colombia Compra Eficiente, el Instituto Nacional Penitenciario y Carcelario INPEC, ha evaluado, tipificado, estimado y asignado provisionalmente los siguientes riesgos previsibles involucrados para la presente contratación, de la siguiente manera:

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	Ejecución	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	la liquidación del contrato	Análisis desde el punto de vista Legal y Financiero.	Mensual
2	Especifico	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	Especifico	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	Ejecución	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	Ejecución	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 la liquidación del contrato	Verificación del cronograma	Permanente

8. GARANTIAS

8.1 GARANTÍA DE CUMPLIMIENTO

El Oferente que resulte adjudicatario debe presentar una garantía de cumplimiento de las obligaciones derivadas del Contrato, a favor del Instituto Nacional Penitenciario y Carcelario INPEC. La garantía de cumplimiento debe tener los siguientes amparos: (A) cumplimiento del Contrato, el cual debe cubrir:(a) el incumplimiento total o parcial del Contrato; (b) el cumplimiento tardío o defectuoso del Contrato; y (c) el pago del valor de las multas y de la cláusula penal pecuniaria; (B) Calidad de los bienes y correcto funcionamiento. La suficiencia de cada uno de los amparos y la vigencia de los mismos es la indicada en la siguiente tabla:

Modalidad	Porcentaje	Vigencia de Amparos
Cumplimiento del contrato	Por el monto equivalente al veinte por ciento (20%) del valor total del contrato	Con una vigencia igual al término de ejecución del mismo y seis (6) meses más, contados a partir de la fecha de suscripción del contrato. En todo caso debe estar vigente para la liquidación del contrato. Este amparo deberá cubrir el pago de las multas que se impongan durante su ejecución y la cláusula Penal según el caso.
Calidad y correcto funcionamiento de los bienes y equipos suministrados	Por el monto de equivalente al veinte (20 %) por ciento del valor del contrato (Este amparo se solicita porque se puede presentar que los equipos y elementos instalados en el transcurso de la garantía no cumplan los parámetros establecidos en el Pliego de Condiciones Definitivo, Contrato y especificaciones técnicas	Con una vigencia igual al término de ejecución del mismo y doce (12) meses más, contados a partir de la fecha de suscripción del contrato.
Calidad del Servicio	Por el veinte por ciento (20%) del valor del contrato. (Se exige este amparo toda vez que se puede presentar que en el servicio de (entrega, implementación y puesta en funcionamiento de la solución de aulas virtuales, en las pruebas de afinamiento de la solución que debe realizar el contratista, en coordinación con los operadores de la solución del INPEC y en la instalación de todos los equipos, no se cumpla.	A partir del momento que se produzca la terminación del contrato y doce (12) meses más.

Pago de Salarios, Prestaciones Sociales e Indemnizaciones laborales	Por el cinco por ciento (5%) del valor total del contrato. (Se constituye este amparo al considerar como riesgo que el contratista no cumpla con el pago a sus empleados)	Por el término de ejecución del contrato y tres (3) años más.
Responsabilidad Civil Extracontractual	Equivalente a (200) SMMLV (Se exige este amparo con el fin de proteger patrimonialmente a la entidad	Con una vigencia igual a la duración del contrato y seis (6) meses más, para cubrir los perjuicios ocasionados por eventuales reclamaciones de terceros derivadas de la responsabilidad extracontractual que surjan de las actuaciones, hechos u omisiones de los subcontratistas autorizados o en su defecto.

El contratista ampliará los plazos iniciales de los amparos en el evento de extenderse el plazo fijado para la ejecución o la liquidación del contrato.

La garantía no podrá ser cancelada sin la autorización expresa y escrita del INPEC.

El CONTRATISTA deberá mantener vigente las garantías, amparos y pólizas a que se refiere esta cláusula y serán de su c
argo el pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, cada vez que se disminuya o agote por razón de las sanciones que se impongan.

Si el CONTRATISTA se demora en modificar las garantías, éstas podrán variarse por la aseguradora o banco a petición del INPEC y a cuenta del CONTRATISTA, quien con la firma del contrato que se le adjudique autoriza expresamente al Instituto para retener y descontar los valores respectivos de los saldos que hubiere a su favor.

NOTA. - EL CONTRATISTA se obliga a ampliar, modificar o prorrogar la garantía única de cumplimiento, en el evento que se aumente el valor del contrato o se prorrogue o suspenda su vigencia.

8.2 GARANTIA DE SERIEDAD DEL OFRECIMIENTO

El Proponente deberá adjuntar a la propuesta, Garantía de Seriedad del Ofrecimiento de conformidad con el artículo 2.2.1.2.3.1.6, del decreto 1082 de 2015, expedida por una Compañía de Seguros legalmente autorizada para funcionar en el país, con las siguientes condiciones:

CUANTÍA: El valor será el equivalente al diez por ciento (10%) del valor total del presupuesto oficial estimado.

VIGENCIA: tres meses (03) contados a partir de la fecha de cierre. Término que se considera de validez de la oferta hasta la aprobación de la garantía que ampara los riesgos propios de la etapa contractual. En todo caso, su vigencia deberá extenderse hasta la aprobación de la garantía que ampara los riesgos propios de la etapa contractual.

TOMADOR O AFIANZADO: Debe figurar como tomador, el nombre completo del Proponente. En caso de presentarse propuesta conjunta, se debe identificar la denominación del consorcio o unión temporal indicando igualmente el nombre o razón social completa de cada uno de sus integrantes con su porcentaje de participación.

BENEFICIARIO: El Instituto Nacional Penitenciario y Carcelario INPEC. Con NIT. 800.215.546-5. De conformidad con el artículo 2.2.1.2.3.1 del Decreto 1082 de 2015, la garantía de seriedad de la oferta se hará efectiva al proponente y cubrirá los perjuicios derivados del incumplimiento del ofrecimiento, en los siguientes casos:

a. La no suscripción del contrato sin justa causa por parte del proponente seleccionado.
b. La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el término previsto en los pliegos para la adjudicación del contrato se prorrogue o cuando el término previsto para la suscripción del contrato se prorrogue, siempre y cuando esas prórrogas no excedan un término de tres meses.
c. La falta de otorgamiento por parte del proponente seleccionado, de la garantía de cumplimiento exigida por la entidad para amparar el incumplimiento de las obligaciones del contrato.
d. El retiro de la oferta después de vencido el término fijado para la presentación de las propuestas.
e. El haber manifestado ser Mipyme para limitar la convocatoria de un proceso contractual sin cumplir los requisitos establecidos en la normativa para tener tal condición.

Nota: Cuando la oferta sea presentada por un Consorcio o Unión Temporal, la garantía debe ser tomada a nombre de todos y cada uno de sus integrantes tal como aparecen en el documento que acredita la existencia y representación legal de cada uno de ellos, especificando el número de identificación de cada uno y su porcentaje de participación en la oferta.

Nota: será causal de rechazo cuando no se presente la seriedad del ofrecimiento junto con la propuesta de acuerdo a lo establecido en el artículo 5, parágrafo 3 de la Ley 1882 del 15 de enero de 2018.

El proponente, por el acto de ofertar, acepta que el INPEC le solicite ampliar el término de vigencia de la garantía de seriedad, cuando haya lugar a ello.

Si el proponente es persona natural y tiene establecimiento de comercio, el tomador deber ser la persona natural y no su establecimiento de comercio.

La suficiencia de esta garantía será verificada por la entidad contratante al momento de la evaluación de las propuestas.

9. ACUERDOS INTERNACIONALES O TRATADOS DE LIBRE COMERCIO

De acuerdo con la definición contenida en el artículo 2.2.2.1.8.5 del Decreto 1082 de 2015, los Acuerdos Comerciales son tratados internacionales vigentes celebrados por el Estado colombiano, que contienen derechos y obligaciones en materia de compras públicas, en los cuales existe como mínimo el compromiso de trato nacional para: (I) los bienes y servicios de origen colombiano y (II) los proveedores colombianos.

EL MANUAL EXPLICATIVO DE LOS CAPÍTULOS DE CONTRATACIÓN PÚBLICA DE LOS ACUERDOS COMERCIALES NEGOCIADOS POR COLOMBIA PARA ENTIDADES CONTRATANTES DEL MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO Y EL DEPARTAMENTO NACIONAL DE

PLANEACIÓN, señala en el anexo 3 que el Instituto Nacional Penitenciario y Carcelario – INPEC es una Entidad Estatal Especial, sin embargo, como Establecimiento Público el INPEC es una entidad Estatal de carácter General.

Acuerdo Comercial		¿Vigente?	Entidad Estatal cubierta	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
		Si/No	Si/No	Si/No	Si/No	Si/No
Alianza Pacífico	Chile	SI	NO	SI	NO	NO
	México	SI	NO	SI	NO	NO
	Perú	SI	NO	NO	NO	NO
Canadá		SI	SI	SI	NO	SI
Chile		SI	SI	SI	NO	SI
Corea		SI	SI	SI	NO	SI
Costa Rica		SI	SI	NO	NO	NO
Estados Unidos		SI	SI	NO	NO	NO
Estados AELC		SI	SI	NO	NO	NO
México		SI	SI	NO	NO	NO
Triángulo Norte	El Salvador	SI	SI	SI	SI	NO
	Guatemala	SI	SI	SI	SI	NO
	Honduras	SI	SI	SI	SI	NO
Unión Europea		SI	SI	NO	NO	NO
Israel		SI	SI	NO	NO	NO
Reino Unido e Irlanda del Norte		SI	SI	NO	SI	NO
Comunidad Andina		SI	NO	SI	NO	NO

NOTA: El acuerdo comercial de Chile es aplicable al presente proceso de contratación por las siguientes razones:

i. El Instituto Nacional Penitenciario y Carcelario, INPEC, hace parte de las entidades del nivel nacional y como establecimiento público es una entidad de carácter General y por ende se encuentra incluida en los citados acuerdos comerciales.

ii. El presupuesto oficial del presente proceso de selección corresponde al valor a partir del cual los citados acuerdos son aplicables.

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