Presidencia	**ESTUDIOS PREVIOS SELECCIÓN ABREVIADA POR SUBASTA INVERSA**

1. DESCRIPCIÓN Y JUSTIFICACIÓN DE LA NECESIDAD:

Son funciones generales del Departamento Administrativo de la Presidencia, según el artículo 4 del Decreto 2647 de 2022, entre otras, las señaladas en los numerales, *"(…) 1. Asistir al Presidente de la República, en su condición de Jefe del Estado, en su labor de coordinación de los diferentes órganos del Estado para que se colaboren armónicamente en la realización de sus objetivos. 2. Organizar, dirigir, coordinar y realizar las actividades necesarias que demande el Presidente de la República, para el ejercicio de las facultades constitucionales que le corresponde ejercer, en relación con los órganos del Estado que integran las ramas del poder público y los demás órganos estatales, autónomos e independientes. (…) 4. Organizar, asistir y coordinar las actividades necesarias que demande el Presidente de la República, para el ejercicio de las facultades constitucionales que le corresponde ejercer como Jefe del Estado y suprema autoridad administrativa. (…) 12. Prestar el apoyo logístico y administrativo que demande el ejercicio de las facultades y funciones presidenciales. (…)"*

Este mismo Decreto, en su artículo 36, establece las funciones de la Oficina de Tecnologías y Sistemas de la Información, destacando principalmente las siguientes:

> *"(…)*
>
> *5. Asesorar al Departamento en la definición de los estándares de datos de los sistemas de información y de seguridad informática.*
> *(…)*
>
> *12. Prestar el soporte técnico básico o de primer nivel a los usuarios internos del Departamento garantizando el adecuado funcionamiento de la infraestructura tecnológica base.*
> *(…)"*

En desarrollo de sus funciones institucionales y de las responsabilidades relacionadas con la gestión, operación y protección de los recursos tecnológicos, el Departamento Administrativo de la Presidencia de la República – DAPRE requiere garantizar la continuidad y fortalecer las capacidades tecnológicas de ciberseguridad destinadas a proteger su infraestructura, la información institucional y los servicios digitales que soportan la operación de la Entidad. Para tal efecto, resulta necesario renovar el licenciamiento de la solución tecnológica de ciberseguridad, junto con los servicios requeridos para su implementación, configuración, soporte y actualización, de manera que se mantengan

operativos los controles de seguridad y se fortalezcan sus capacidades frente a la evolución de las amenazas y a las necesidades actuales del entorno tecnológico institucional.

La renovación de la solución resulta necesaria para preservar la continuidad de los mecanismos de protección aplicados sobre los diferentes componentes de la infraestructura tecnológica y evitar la pérdida o disminución de las capacidades institucionales de prevención, detección, investigación y respuesta ante incidentes de seguridad. A su vez, permite fortalecer los controles existentes mediante funcionalidades que proporcionen mayor visibilidad, correlación y capacidad de actuación frente a eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información o afectar la continuidad de los servicios tecnológicos.

La infraestructura tecnológica institucional comprende estaciones de trabajo, servidores, correo electrónico, datos, sistemas de información y cargas de trabajo, los cuales se encuentran expuestos a amenazas conocidas, desconocidas y emergentes. En consecuencia, la continuidad de su protección requiere disponer de mecanismos que permitan prevenir, detectar, analizar, investigar, contener y remediar amenazas, proporcionando información suficiente sobre los eventos de seguridad, su contexto y posible impacto, de manera que se facilite la adopción oportuna de acciones de mitigación y respuesta.

En este sentido, la necesidad no se circunscribe a la renovación de funcionalidades tradicionales de antivirus, sino a mantener y fortalecer una solución tecnológica integral de ciberseguridad que articule capacidades de protección antimalware, detección y respuesta EDR y XDR, prevención de pérdida de información (DLP), protección de servidores, parchado virtual, seguridad del correo electrónico, inteligencia de amenazas, administración centralizada e interoperabilidad con la infraestructura tecnológica de la Entidad.

Como parte de esta renovación, se requiere mantener y fortalecer las capacidades de protección antimalware, orientadas a prevenir, identificar, analizar, bloquear y contener amenazas tales como virus, troyanos, gusanos, spyware, ransomware, exploits y demás tipos de código malicioso, incluyendo amenazas conocidas y desconocidas. Estas capacidades deben complementarse con mecanismos de análisis de comportamiento, aprendizaje automático, inteligencia de amenazas y análisis dinámico, que permitan mejorar la identificación y el tratamiento oportuno de comportamientos potencialmente maliciosos.

Así mismo, la renovación debe mantener y fortalecer las capacidades de detección y respuesta EDR/XDR, prevención de pérdida de información (DLP) y protección de servidores, permitiendo identificar, correlacionar, investigar y responder ante amenazas, prevenir la fuga o transferencia no autorizada de información y reducir la exposición frente a código malicioso y explotación de vulnerabilidades. Para los servidores, estas capacidades se complementarán con parchado virtual, como mecanismo adicional de protección mientras se realizan los procesos de validación y aplicación de actualizaciones.

De igual manera, se requiere garantizar la continuidad de la protección del correo electrónico institucional para 2.300 cuentas, frente a amenazas como spam, phishing, suplantación, malware y ransomware, mediante el análisis de mensajes, remitentes, enlaces y archivos adjuntos y la aplicación de acciones de seguridad como alertamiento, bloqueo y cuarentena. Estas capacidades deberán operar de forma integrada con los demás componentes de seguridad, facilitando la correlación, investigación y respuesta ante incidentes que puedan afectar el entorno tecnológico institucional.

En concordancia con el carácter integral de la solución que se pretende renovar, resulta igualmente necesario preservar y fortalecer su capacidad de integración e interoperabilidad con la infraestructura tecnológica institucional y con las demás herramientas de seguridad de la Entidad, evitando la operación aislada de los controles y facilitando el intercambio de información requerido para los procesos de monitorización, detección, análisis, investigación y respuesta.

Para ello, la solución debe disponer de mecanismos de integración basados en estándares, interfaces y protocolos documentados que permitan su articulación, según corresponda, con servicios de identidad y directorio, herramientas de gestión de eventos de seguridad, plataformas de automatización y respuesta, servicios de inteligencia de amenazas, herramientas de gestión de vulnerabilidades y demás componentes tecnológicos que integren el ecosistema institucional.

Esta interoperabilidad, acompañada de capacidades de administración centralizada, permitirá consolidar y correlacionar información procedente de diferentes capas de protección, facilitando la gestión de políticas, roles, usuarios, dispositivos, alertas, eventos e incidentes de seguridad, así como la obtención de información y reportes para el seguimiento de las condiciones de seguridad del entorno tecnológico.

Estos servicios son necesarios para asegurar que los diferentes componentes y controles de seguridad operen de forma adecuada y articulada, conforme con las características de la infraestructura de la Entidad, así como para disponer del acompañamiento técnico

requerido ante situaciones que puedan afectar el funcionamiento de la solución o sus capacidades de protección.

La renovación de la solución se encuentra igualmente asociada al fortalecimiento de la gestión de seguridad y privacidad de la información y de los riesgos de seguridad digital. La continuidad de estos controles tecnológicos contribuye a prevenir, detectar, investigar y responder frente a eventos que puedan comprometer los activos de información, y apoya la aplicación de las políticas institucionales de seguridad y privacidad de la información y la gestión de los riesgos asociados al entorno tecnológico.

De igual manera, mantener capacidades integradas de protección, prevención, detección, investigación, contención y respuesta contribuye a fortalecer la continuidad y resiliencia de los servicios tecnológicos, al reducir la exposición y el posible impacto de incidentes relacionados, entre otros, con código malicioso, explotación de vulnerabilidades, accesos no autorizados, ransomware, pérdida o fuga de información y amenazas asociadas al correo electrónico.

Asimismo, la contratación se encuentra incluida en el Plan Anual de Adquisiciones – PAA de la Entidad, como parte de las acciones orientadas al fortalecimiento de la infraestructura tecnológica y de las capacidades institucionales de seguridad de la información y ciberseguridad.

En consecuencia, resulta necesario renovar el licenciamiento de la solución tecnológica integral de ciberseguridad, junto con los servicios de implementación, configuración, soporte y actualización asociados, con el propósito de garantizar la continuidad de los controles tecnológicos actualmente requeridos por la Entidad y fortalecer sus capacidades de prevención, protección, detección, investigación, contención y respuesta frente a amenazas cibernéticas. Con ello se busca mantener la protección de las estaciones de trabajo, servidores, correo electrónico, datos y cargas de trabajo; fortalecer la prevención de pérdida o fuga de información; reducir la exposición frente a la explotación de vulnerabilidades; y contribuir a preservar la confidencialidad, integridad y disponibilidad de la información y la continuidad de los servicios tecnológicos que soportan el cumplimiento de las funciones del Departamento Administrativo de la Presidencia de la República – DAPRE.

JUSTIFICACIÓN DE LA RENOVACIÓN Y LA MARCA. En el marco del análisis de conveniencia, la Entidad adelantó la solicitud de información a proveedores DAPRE-SIP-2026-EDR_ANTISPAM_DLP, con el propósito de conocer las condiciones económicas del mercado para una solución integral de protección de endpoints (Antivirus/EDR), seguridad

de correo electrónico (Antispam) y prevención de pérdida de datos (DLP). Como resultado se recibieron seis (6) propuestas económicas, cuyo promedio asciende a $3.528.923.488,50.

Al comparar dicho promedio con el valor estimado para la renovación de la solución tecnológica actualmente implementada, se evidencia que las alternativas consultadas representan, en promedio, un valor aproximadamente 5 veces superior, equivalente a un incremento del 500% frente al valor de la renovación.

En consecuencia, la renovación y continuidad de la solución actualmente implementada se sustenta en criterios técnicos, operativos y económicos y no en una mera preferencia tecnológica, toda vez que permite mantener y fortalecer las capacidades institucionales de ciberseguridad, preservar la continuidad de los controles existentes y optimizar los recursos públicos. El sondeo de mercado evidencia que la sustitución por una solución integral alternativa implicaría un costo sustancialmente mayor, por lo que la renovación constituye una alternativa económicamente más eficiente para satisfacer la necesidad institucional.

2. OBJETO A CONTRATAR:

Contratar la renovación del licenciamiento, implementación, configuración, soporte y actualización de la solución integral de ciberseguridad para la protección, detección, investigación y respuesta frente a amenazas en estaciones de trabajo, servidores, correo electrónico, datos y cargas de trabajo de la Entidad, con capacidades de antimalware, EDR/XDR, DLP, parchado virtual e integración con la infraestructura tecnológica institucional.

3. FICHA TÉCNICA Y ESPECIFICACIONES TÉCNICAS

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
La solución de antimalware deberá cumplir con mínimo los siguientes requerimientos:
1. Análisis de comportamiento dinámico detectando patrones anómalos en archivos, aplicaciones y tráfico de red antes de que se conviertan en amenazas activas.
2. Prevención contra exploits, malware conocido y desconocido, virus, troyanos, gusanos, rootkits, Spyware/Grayware, Ransomware, CVE exploit, Fileless como PowerShell malicioso o macros malintencionadas, Cryptojacking, APT, wipers, entre otros.
3. Identificación, análisis y bloqueo de archivos maliciosos, basado en el tipo de archivo real y verdadero, no solo en la extensión de archivo.
4. Identificación y bloqueo de archivos basados en contenido ejecutable incrustado o script.
5. Identificación análisis y bloqueo de procesos y archivos asociados a ataques de Ransomware

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
6. Uso de modelos predictivos de aprendizaje automático y análisis de comportamiento para identificar el comportamiento anómalo sobre archivos y procesos que buscan modificar/afectar el sistema o generar tareas de persistencia
7. Protección en tiempo de ejecución para detectar y bloquear el comportamiento de cifrado malicioso en tiempo real, incluso en variantes de ransomware desconocidas.
8. Bloqueo de ransomware multi-etapa detectando cadenas de ataque que involucran múltiples técnicas, como el cifrado selectivo combinado con exfiltración de datos.
9. Restauración de archivos cifrados usando copias de seguridad automáticas (de archivos críticos) generadas en tiempo real para restaurar sistemas afectados.
10. Configuración independiente para escaneo y protección frente amenazas en Tiempo Real, escaneo Manual, escaneo Programado o escaneo enviado por el administrador.
11. Definición manual o recomendada de acciones sobre la identificación de amenazas, como enviar a cuarentena, eliminar, bloquear la acción o generar log
12. Uso de servicios de remediación y limpieza automática definidos y soportados por el fabricante de la solución ofertada
13. Configuración de excepciones por directory path, Files o Extensions
14. Protección frente amenazas incluso si el agente pierde la conexión a la consola de gestión
15. Protección contra intentos de desinstalación o eliminación de procesos del agente de protección.
16. Identificación sobre archivos comprimidos o que intentan generar ataques conocidos como bombas zip
17. Uso de servicio global de inteligencia de amenazas para la actualización en tiempo real sobre nuevas amenazas o factores de riesgo a nivel global.
18. Capacidad de Web Reputation sobre la navegación de los usuarios
19. Configuración de uso de CPU sobre los dispositivos
20. Capacidad de correlación automática de datos entre múltiples capas integrando información de endpoints, servidores, red, correo electrónico, servidores y cargas de trabajo en la nube para ofrecer una visión centralizada y holística de las amenazas.
21. Uso de modelos de correlación incluidos y soportados por la solución ofertada, con posibilidad de generar modelos de correlación personalizados.
22. capacidad de verificar el perfil de ejecución/análisis de causa raíz (perfil de ejecución y análisis de causa raíz) para ver las acciones que una amenaza llevó a cabo en el endpoint.
23. Capacidad de aislar un dispositivo si es identificado como el "Paciente cero" que propaga la amenaza
24. Conexión por shell remota al dispositivo para un análisis adicional sobre la amenaza o afectación en el sistema
25. Posibilidad de generar casos asignados a diferentes analistas que generan los procesos de investigación
26. Línea de tiempo de cada evento relacionado con la amenaza que fue identificada y correlacionada

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
27. Posibilidad de documentar cada investigación realizada por el analista directamente en la plataforma de la solución ofertada
28. Posibilidad de modificar el estado del evento o correlación generada a un estado en proceso, cerrado, falso positivo, verdadero positivo, entre otros
29. Descripción detallada de correlación generada incluyendo, línea de tiempo, mapeo directo con el framework de MITRE ATT&CK, comandos usados, rutas de ejecución, archivos o elementos usados, conexiones de red, entre otros
30. Posibilidad de tomar acciones de remediación automática o manual a través de Playbook. Acciones como aislar el dispositivo, iniciar un shell remoto, generar una búsqueda adicional con un criterio especifico, ejecutar script personalizados, ejecutar un OSquery, ver el detalle del dispositivo o elemento identificado, entre otros.
31. Posibilidad de ver activos adicionales que están relacionados con el dispositivo que fue identificado con un evento anómalo
32. Uso asistente virtual por medio de IA generativa que permite ayudar a los equipos de seguridad a interpretar de mejor forma cada amenaza identificada además de recomendaciones que se pueden ejecutar
33. Sección específica para el análisis de técnicas tácticas y procedimientos basados en MITRE ATT&CK
La solución debe contar con una consola centralizada que cumpla con mínimo las siguientes características:
34. Capacidad retención mínima para log de seguridad de 180 días, telemetría por 30 días y eventos correlacionados por 180 días
35. Funcionalidad para crear roles granulares por sección para la asignación a usuarios específicos.
36. Integración con directorios y servicios de identidad locales o en la nube mediante SAML 2.0, OIDC, OAuth 2.0, LDAP o LDAPS para uso de autenticación centralizada a la plataforma de gestión usando SAML
37. Uso de IA para generar recomendaciones de configuración y acciones de remediación.
38. Posibilidad de restringir el acceso a la plataforma de gestión a direcciones de IP específicas
39. Gestión centralizada para diferentes tenant o compañías del mismo grupo en una única consola de administración
40. Integración con soluciones de terceros como:
• Seguridad de red: capacidad de integración con los controles de red de la Entidad mediante Syslog, CEF, APIs documentadas, STIX/TAXII u otros mecanismos estándar.
• SIEM: capacidad de integración mediante Syslog, CEF, LEEF, API documentada u otros formatos estándar, incluyendo la plataforma institucional.
• SOAR: capacidad de integración mediante API documentada, webhooks, conectores estándar o mecanismos equivalentes.
• Gestión de servicios de TI: capacidad de integración mediante API documentada, correo, webhooks o conectores estándar.

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
• Inteligencia de amenazas: compatibilidad con STIX/TAXII, MISP u otros formatos y fuentes interoperables.
• Simulación de brechas y ataques: integración mediante API documentada o conectores compatibles con las herramientas disponibles en la Entidad.
a. Gestión de identidades y accesos: integración con servicios de directorio e identidad locales o en la nube mediante LDAP/LDAPS, SAML 2.0, OIDC, OAuth 2.0 o API documentada, permitiendo correlacionar el comportamiento de los usuarios con la telemetría de seguridad.
b. Gestión de vulnerabilidades: capacidad de integración mediante API documentada, archivos estructurados o conectores con herramientas de gestión de vulnerabilidades reconocidas.
41. API disponible para ejecutar diferentes acciones de administración, reportes, configuración, IoC, Integración con terceros, entre otros
42. El esquema de licenciamiento deberá ser flexible y permitir habilitar las capacidades requeridas, mediante suscripción, licencias por activo, consumo, créditos u otra modalidad equivalente, indicando claramente métricas, límites y costos.
43. Posibilidad de aplicar controles de seguridad a los agentes de protección para evitar su desinstalación o eliminación de procesos activos
44. Integración con soluciónes de SIEM y SOAR para el envío de logs
Protección contra amenazas en los servidores:
Requerimientos técnicos Generales
Licenciamiento de la protección anti-malware para mínimo 300 servidores.
La solución debe brindar protección para mínimo los siguientes sistemas operativos:
• Windows Server, en versiones vigentes o heredadas que la Entidad mantenga en operación y que sean declaradas compatibles por el fabricante.
• Linux, para la versión distribuciones empresariales de Linux en versiones soportadas o heredadas declaradas compatibles por el fabricante.
• Linux para la versión distribuciones comunitarias de Linux en versiones soportadas o heredadas declaradas compatibles por el fabricante.
• Linux en sus diferentes distribuciones.
• Validar con Infraestructura las diferentes distribuciones.
• La solución debe detectar, identificar y contener malware.
La solución debe realizar protección en tiempo real contra malware.
1. Posibilidad de almacenamiento de eventos correlacionados por 180 días
2. Sección específica para la creación de consultas personalizadas enfocadas en threat hunting sobre la telemetría recopilada por los agentes, usuarios, correo y servidores
3. Posibilidad de construir, guardar y reutilizar búsquedas para Threat Hunting
4. Posibilidad de generar consultas con atributos de búsqueda, operadores y valores especificados en una única consulta de búsqueda.
5. Permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios de búsqueda
6. Resultados de búsquedas con posibilidad de exportar a CSV o JSON

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
7. Posibilidad de notificar o alertar un match con una búsqueda o filtro personalizado, en un periodo de tiempo
8. Escaneo de recomendaciones y asignación de reglas automáticamente, identificando y bloqueando únicamente el tráfico malicioso.
9. Asignación de reglas por política genera par aun grupo de dispositivos o por host independiente
10. Posibilidad de generar escaneos de recomendaciones y reportes de reglas de vulnerabilidades aplicadas y recomendadas para aplicar, además de reglas disponibles según la vulnerabilidad
11. La solución deberá disponer oportunamente de reglas de parchado virtual para vulnerabilidades críticas publicadas por los fabricantes de los sistemas operativos y aplicaciones soportados.
12. Protección de intentos de explotación de vulnerabilidades sobre el tráfico de red del dispositivo
13. Despliegue de reglas de Virtual Patch sin necesidad de reinicio del dispositivo
14. Soporte para proteger vulnerabilidades sobre sistemas legados como sistemas operativos vigentes y heredados inventariados por la Entidad, o distribuciones de Linux
15. Inspección profunda de paquetes bidireccionalmente para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades conocidas y de día cero
16. Capacidad de aplicar reglas con acciones de bloqueo y monitoreo, además, poder capturar el stream o la cadena de caracteres de la ejecución de un ataque que permita el análisis del evento y alertamiento.
17. Protección adicional frente ataques de tipo SQL Injection, Cross-Site Scripting y otras vulnerabilidades de aplicaciones web
18. Capacidad de realizar escaneos de recomendaciones bajo demanda y programados, sin límite de escaneos, para detectar vulnerabilidades relacionadas con la plataforma (sistema operativo, aplicativo de servidor web y aplicativo de servidor de aplicaciones) sobre la cual están montados los sitios web expuestos a Internet
19. Capacidad de crear reglas de Firewall que protege servidores físicos, y/o virtuales y/o en la nube administrados desde la misma plataforma, permitiendo sólo las comunicaciones requeridas entre ellos. Filtrado bidireccional ICMP, IGMP, GGP, TCP, PUP, UDP, IDP, ND, RAW, TCP+UDP, Direcciones MAC, Direcciones IP y Puertos TCP & UDP entre otros
20. Posibilidad de reconocer y bloquear direcciones IP que estén realizando escaneos de reconocimiento, port scan, TCP Null Scan, TCP SYNFYN Scan, TCP Xmas Scan por hasta 30 minutos.
21. Asignación de reglas por política general, por dispositivo o por interfaz
22. La solución deberá incluir un catálogo actualizado de reglas predefinidas de monitoreo de integridad para sistemas operativos y aplicaciones, además de permitir reglas personalizadas para detectar cambios no autorizados en rutas críticas.

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
23. Posibilidad de crear políticas personalizadas de File Integrity Monitoring para monitorear rutas críticas, archivos, o carpetas, definiendo la severidad, rutas o archivos a monitorear y excepciones de las mismas
24. Permite generar un monitoreo de integridad, en tiempo real, programado o a demanda
25. Permite la creación de una línea base del servidor, modificación o actualización de esta al crear o agregar nuevas rutas o archivos que serán monitoreadas
26. Cuenta con un escaneo de recomendaciones que permite aplicar reglas automáticamente acordes al sistema operativo o aplicaciones identificadas en el sistema, para File Integrity Monitoring y Log Inspection.
Protección DLP
Licenciamiento de la protección DLP para mínimo 2400 endpoints.
La solución debe tener un componente de prevención de fuga de información a nivel de Endpoint incluido en el mismo agente de protección antimalware.
La solución debe brindar protección DLP a nivel de datos o información con mínimo las siguientes funcionalidades:
• Monitoreo y protección a partir de diccionarios o palabras clave.
• Implementar políticas de detección y protección.
• Permitir la implementación de políticas para la protección de los archivos almacenados en los Endpoint de la Entidad.
• Detectar y prevenir intentos de copia o cifrar datos de manera no autorizada.
1. La solución debe tener la capacidad de prevenir y/o informar sobre la fuga o perdida de información sensible de la organización ya sea de forma accidental o deliberada.
2. La solución debe permitir identificar o configurar los activos digitales que se desean proteger.
3. La solución debe permitir la creación de políticas que limiten la transmisión o transferencias de activos digitales por los canales de comunicación convencionales (email y/o dispositivos externos).
4. La solución debe tener la capacidad de igualmente brindar protección y aplicar políticas para transferencia de activos digitales mediante cliente de correo ya será software o web.
5. La solución debe permitir que la organización haga cumplir con las normas de privacidad establecidas.
6. La solución debe tener la capacidad de brindar protección contra filtrado de datos sensibles y proporcionar un control de dispositivos, permitiendo configurar reglas o políticas para ser aplicadas a grupos o agentes individuales.
7. La solución debe proporcionar identificadores de datos y/o plantillas para la creación de políticas.
8. La solución debe tener la capacidad de identificar o reconocer archivos ejecutables, documentos, gráficos vectoriales, archivos multimedia, archivos comprimidos, bases de datos, hojas de cálculo, presentación, archivos vinculados e incrustados, y/o archivos encriptados.

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
9. La solución debe tener la capacidad de localizar activos digitales almacenados en portátiles, equipos de escritorio, y servidores.
10. La solución debe tener la capacidad de proporcionar filtros de protección para canales de red como FTP o HTTP, canales de aplicaciones o periféricos.
11. La solución debe tener la capacidad de detectar datos estructurados y no estructurados.
12. La solución debe mantener un monitoreo constante.
13. La solución debe proveer plantillas que permitan el cumplimiento de estándares como GLBA, HIPAA, PCI-DSS o PII.
14. La solución debe permitir la integración con servicio de directorio institucional y permitir la delegación de administración.
15. La solución debe contar con una consola de administración WEB que permita la configuración de políticas e implementaciones, reportes de los equipos, extracción de huellas digitales, y actualizaciones.
16. La solución debe contar con una herramienta que analice los activos digitales que se encuentran almacenados en los portátiles o computadores de escritorio aun así no estén conectados en la red de la organización.
17. La solución debe tener la capacidad de identificar los activos digitales almacenados en los dispositivos o el tráfico en la red utilizando expresiones regulares (predefinidas y/o personalizadas), atributos de archivos (tipo y/o tamaño), huellas digitales, palabras clave, y/o plantillas (predefinidas y/ personalizadas)
18. Las plantillas de identificación de activos digitales deben permitir combinar identificadores de datos (expresiones, atributos de archivos, huellas digitales, lista de palabras).
19. La solución debe permitir usar plantillas predefinidas por el fabricante, personalizarlas, crear plantillas, importar plantillas, exportar plantillas, y eliminar las plantillas.
20. La solución debe permitir implementar políticas independientes tanto para agentes fuera de la red corporativa como para agentes dentro de la red.
21. La solución debe permitir generar reportes ya sea por demanda o de forma programada (Diario, semanal o mensual), estos reportes deben contener información de los logs de los agentes. Dichos reportes deben mostrar información relevante como top de incidentes, información resumida, reporte de auditoría, entre otros.
22. La solución debe permitir almacenar reportes y estos deben estar disponibles en formatos PDF, HTML, o Microsoft Excel.
23. La solución debe tener la capacidad de administrar los logs de manera que pueda eliminar los Logs que tengan un tiempo de más de 180 días, igualmente debe permitir la realización de una copia de seguridad y limpieza de los mismos de forma manual.
24. La solución debe permitir que las actualizaciones puedan ser implementadas en ambientes de pruebas y producción para validar el funcionamiento de estos.
25. La Solución debe tomar acción como mínimo en documentos y métodos de codificación, Gráficos, Archivos multimedia, Archivos comprimidos, Bases de datos, Hojas de cálculo, Archivos de presentaciones y diagramas, Archivos vinculados e incrustados, Archivos cifrados, cuando técnicamente sea posible.

REQUERIMIENTOS TÉCNICOS MÍNIMOS:
dBase (.dbf), Microsoft Access (.mdb, .accdb), KIRI Database (.tbl), SAS System Data Set (.sas7bdat), Bitmap (.bmp), EPS (.eps), GIF (.gif), TIFF (.tif), JPEG (.jpg), PNG (.png), DICOM (.dcm), PostScript (.ps), AutoDesk (.dwg), AutoCAD (.dxf), SolidWorks (.abc, .slddrw, .sldprt, .sldasm), Siemens NX Unigraphics (.prt), CATIA (.CATDrawing, .CATPart, .CATProduct), Graphic Data System (.gds), Lotus Ami Pro (.sam), RTF (.rtf), Microsoft Word for Windows - Non-encrpyted (.doc, .dot, .docx, .dotx, .docm, .dotm), WordPerfect (.wp, .wpd), WordStar (.wsd), Microsoft Write (.wri), Adobe PDF - Non-encrypted (.pdf), HTML (.htm), XML (.xml), Xerox DocuWorks (.xdw, .xbd), Ichitaro (.jtd), Microsoft Wave (.wav), MIDI (.mid), AVI (.avi), MPEG (.mpeg), Apple QuickTime (.mov), Adobe Flash (.swf), Zipped File (.zip) PAK/ARC (.arc), compress (.Z), GZ (.gz), TAR (.tar), MIME (.eml), PGP Keyring (.pgp) Microsoft Outlook (.pst), RAR (.rar), LHA (.lzh), Microsoft Outlook Express (.dbx), ARJ (.arj), bzip2 (.bz2), Microsoft Compiled HTML Help (.chm), Microsoft Outlook (.msg) 7-Zip (.7z), Quattro (.qpw, .wb3, .wb2, .wb1, .wq1), Lotus 1-2-3 (.123, .wk1, .wk3, .wk4, .wke, .wks), Microsoft Excel - Non-encrypted (.xls, .xlw, .xlsx, .xltx, .xlsb, .xltm, .xlsm, .xlc, .xlam), Microsoft PowerPoint for Windows - Non-encrypted (.ppt, .pot, .pps, .pptx, .potx, .ppsx, .potm, .pptm, .ppsm), Microsoft Visio (.vdx, .vsd, .vss, .vst, .vsx, .vtx, .vdw), OLE (.ipt, .idw, .iam, .pqw, .msoffice), Encrypted compressed files (.rar, .zip), Encrypted documents (.accdb, .doc, .docx, .pdf, .ppt, .pptx, .wb1, .wb2, .wq1, .wpd, .xls, .xlsx)
26. La herramienta de análisis local debe tener la capacidad de adquirir huellas digitales para los archivos almacenados en el equipo.
27. La solución provee expresiones predefinidas para los números de tarjetas de crédito. A estos números se les realiza una verificación adicional por el número de prefijo, y verificación con LUHN.
28. La solución provee expresiones predefinidas para las direcciones de correo electrónico
29. La solución provee expresiones predefinidas para los números de cuentas de bancos internacionales (IBAN).
30. La solución provee expresiones predefinidas para códigos de identificación de negocio SWIFT BIC.
31. La solución deberá proveer una lista de palabras predefinidas para la validación de formularios como fecha de nacimiento, fecha de expiración, Nombres y apellidos, lugar de nacimiento, departamentos o ciudades y direcciones de domicilios.
32. La solución debe proveer una lista de palabras que pueden ser usadas en contextos efectivos, racistas o que incluyan elementos para causar daño (armas)
33. La solución deberá proveer una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.
Protección XDR
Licenciamiento de la protección XDR para mínimo 300 servidores y 2400 endpoints
La solución debe permitir identificar, investigar y responder a amenazas avanzadas de manera automatizada.
La solución debe integrarse y correlacionarse con el SIEM institucional mediante Syslog, CEF, API documentada u otro mecanismo estándar disponible

REQUERIMIENTOS TÉCNICOS MÍNIMOS:	
La solución podrá utilizar uno o más agentes, siempre que estén integrados, sean administrados centralmente y no generen incompatibilidades, duplicidad innecesaria de consumo de recursos ni afectación significativa del desempeño.	
La solución XDR deberá aprovechar la telemetría de los agentes de protección instalados o integrarse con ellos mediante mecanismos documentados. Si requiere componentes adicionales, el oferente deberá indicar su función, consumo de recursos y método de administración centralizada.	
La solución de detección y respuesta debe permitir la correlación entre, endpoints y los servidores protegidos por la solución XDR o integrados mediante mecanismos documentados e interoperables	
Integración con las plataformas de seguridad e infraestructura de la Entidad mediante estándares abiertos y mecanismos documentados, como Syslog, CEF, STIX/TAXII, SAML 2.0, OIDC, LDAP/LDAPS, API REST y webhooks. El oferente deberá indicar las integraciones nativas disponibles y el procedimiento para desarrollar o habilitar integraciones adicionales.	
Integración con el servicio de directorio institucional para identificación de comportamiento maliciosos sobre los usuarios que alteren el nivel de riesgo por relación a una posible amenaza o brecha de datos	
Capacidad de deshabilitar el usuario, forzarlo a un cierre de sesión y forzar el reseteo de la contraseña si es identificado con comportamiento malicioso	
Protección completa contra Phishing, Spam, Graymail, Malware Avanzado con múltiples técnicas de protección, incluyendo análisis del remitente, de contenido e imágenes usando Machine Learning	
Protección completa contra Phishing, Spam, Graymail, Malware Avanzado con múltiples técnicas de protección, incluyendo análisis del remitente, de contenido e imágenes usando Machine Learning	
La solución deberá incluir protección antispam para los servidores de correo Microsoft Exchange Server de la Entidad, con capacidad de inspeccionar y filtrar el correo electrónico interno entre buzones del mismo dominio, además del correo entrante y saliente.	
La protección deberá analizar mensajes, remitentes, encabezados, contenido, URL y archivos adjuntos, mediante técnicas de reputación, reglas, análisis de contenido, aprendizaje automático u otros mecanismos equivalentes, con el fin de detectar spam, phishing, suplantación, malware y mensajes no deseados.	
La solución deberá permitir aplicar políticas diferenciadas al flujo de correo interno, entrante y saliente, con acciones configurables como permitir, etiquetar, bloquear, rechazar, eliminar o enviar a cuarentena.	
La solución deberá integrarse con Microsoft Exchange Server mediante agentes de transporte, conectores, diario de correo, API, gateway interno u otro mecanismo oficialmente soportado. El oferente deberá describir la arquitectura propuesta y demostrar que el correo interno será efectivamente inspeccionado.	
Advanced Email Protection - 2300 cuentas de correo	
La solución deberá tener la capacidad para proteger correos entrante, saliente, internos, de la organización sobre la plataforma Google Workspace, O365, Exchange, entre otros	
La solución deberá proporcionar cuarentena administrable, listas de permitidos y bloqueados, excepciones, trazabilidad de mensajes, reportes y registros de auditoría para la protección antispam.	

REQUERIMIENTOS TÉCNICOS MÍNIMOS:	
La solución debe tener la capacidad de detección de correos internos que suplantan a usuarios de alto perfil (ejecutivos) o provienen de cuentas comprometidas.	
La solución deberá analizar el contenido de los correos internos, los cuales no salen a internet, con filtros antispam ajustables, con cuarentena de usuario final y nivel de confianza de spam.	
La solución deberá permitir aplicar controles contra suplantación de identidad y spoofing interno, incluyendo validaciones de remitente, dominio y autenticidad del mensaje cuando sean aplicables.	
Protección completa contra Phishing, Spam, Graymail, Malware Avanzado con múltiples técnicas de protección, incluyendo análisis del remitente, de contenido e imágenes usando Machine Learning	
Detectar y bloquear ransomware y otros tipos de malware de día cero que llegan por correo mediante machine learning previo a la ejecución, análisis de macro, detección de exploit y análisis dinámico en sandbox para archivos y URL	
La solución deberá permitir el despliegue mediante API documentada, integración con el flujo de correo o mecanismos equivalentes, indicando los cambios técnicos requeridos.	
La solución podrá ofrecerse en modalidad SaaS, local o híbrida, siempre que cumpla los requisitos de seguridad, disponibilidad, administración y protección de datos de la Entidad.	
Detectar malware avanzado y exploits en archivos PDF, Microsoft® Office y otros documentos a través de la lógica estática o heurística para detectar y examinar anomalías	
La solución debe contar con fuentes de inteligencia del fabricante que permita tener información sobre amenazas, para correlacionar registros de Internet, emails, archivos, dominios y muchas otras fuentes de amenazas para identificar las infraestructuras del atacante antes de que se ejecuten	
La solución deberá tener Sandbox para análisis de amenazas desconocidas y ataques de día cero.	
La solución deberá tener escaneo de URL en el cuerpo de los correos y en los archivos adjuntos.	
La solución deberá ofrecer protección avanzada para los servicios institucionales de almacenamiento y colaboración en la nube.	
La solución deberá admitir conectores o API documentadas para servicios de almacenamiento y colaboración en la nube utilizados por la Entidad.	
La solución deberá tener DLP y plantillas customizables para controlar la fuga de información permitiendo realizar pruebas de expresiones regulares y listados de palabras para nuevas plantillas	
La solución deberá tener DLP a nivel de Email con la capacidad de descubrir y reportar violaciones a las políticas.	
La solución deberá aplicar capacidades DLP a los servicios de almacenamiento y colaboración en la nube integrados, detectando y reportando incumplimientos de políticas.	
La solución no deberá exceder 1 minuto de latencia.	
La solución deberá ofrecer disponibilidad del servicio superior a >99%.	
Integración para autenticación de administradores con servicios de identidad locales o en la nube mediante SAML 2.0, OIDC u otro estándar equivalente, con soporte de autenticación multifactor.	
La solución deberá tener la capacidad desde la consola en la nube, de crear políticas basadas en reglas según el correo entrante o saliente y a los cuales se les pueda personalizar las acciones a tomar en categorías de (Clean, Delete, Tag, encriptar, notificar).	

REQUERIMIENTOS TÉCNICOS MÍNIMOS:	
La solución deberá tener la capacidad en la consola en la nube de mostrar distintos gráficos para dar seguimiento al tráfico de correo y cuarentenas.	
La solución deberá tener la capacidad en la consola en la nube de habilitar a los usuarios finales la capacidad de aprobar remitentes para sacarlos de cuarentena.	
La solución deberá tener la capacidad de analizar los enlaces que se encuentren en el cuerpo del mensaje de los correos electrónicos, igualmente debe tener la capacidad de analizar los enlaces que se encuentren ocultos en el cuerpo del mensaje, ya sea en botones, banners o imágenes en el momento en el que el usuario le de clic en el enlace	
La solución deberá tener la capacidad en la consola en la nube de reportar ataques dirigidos.	
La solución deberá permitir la aplicación de reglas de forma granular es decir que dichas políticas puedan ser aplicadas a cuentas de usuario especificas o elementos del correo.	
La solución debe proporcionar seguridad para la información que se encuentra almacenada en la nube y garantizar la privacidad de la misma.	
La solución debe tener la capacidad de identificar amenazas que aun no han sido reportadas con el análisis de los archivos.	
La solución debe proporcionar proteccion avanzada contra ataques de BEC (Business Email Compromise) con el análisis de los mensajes y usando tecnicas de aprendizaje de estilos de escritura.	
La solución debe tener la capacidad de detectar ataques dirigidos mediante explotacion de archivos.	
La solución debe tener la capacidad de realizar un análisis avanzado de los archivos usando Machine Learning, para identificar amenazas que aun no han sido reportadas, pero que pueden generar una afectacion sobre los datos o el sistema que esta utilizando el usuario.	
La solución debe tener la capacidad de brindar proteccion contra ataques avanzados como Business Email Compromise (BEC), Ransomware, Phishing avanzado	
La solución debe tener la capacidad de tomar un accion sobre los correos que sean identificados como spam avanzado, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una etiqueta al asunto del correo.	
La solución debe tener la capacidad de tomar un accion sobre los correos que sean analizados con el sandbox y sean identificados como maliciosos o sospechosos, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una etiqueta al asunto del correo.	
La solución deberá permitir aplicar acciones sobre archivos almacenados en servicios de colaboración en la nube que sean identificados como maliciosos, sospechosos o contrarios a las políticas, incluyendo permitir, bloquear, eliminar, poner en cuarentena y notificar al usuario.	
La solución debe tener la capacidad de notificar al usuario cuando algun correo que iba dirigido a el tuvo alguna accion reactiva, basado en las reglas configuradas, dicha notificacion debe indicarle que accion se tomo sobre el correo que iba dirigido a el y la razon de esta.	
La solución debe permitir a los administradores configurar la lista de excepciones, de los archivos detectados mediante Machine Learning como maliciosos o sospechosos.	
La solución debe permitir restaurar archivos que sean enviados a cuarentena ya sea por fueron detectados como maliciosos o que no cumplen con las políticas de Prevencion de filtracion de datos de la organización.	

REQUERIMIENTOS TÉCNICOS MÍNIMOS:	
Debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos correlacionados.	
La solución debe permitir realizar un escaneo manual en modo de evaluacion para permitir a los administradores verificar las reglas que seran aplicadas para proteger la plataforma de correo y colaboración en la nube de la Entidad sin tomar ninguna accion sobre dichos correos o archivos.	
Envío de registros al SIEM mediante Syslog, CEF, API documentada u otro mecanismo estándar e interoperable.	
Creación de usuarios y roles personalizados con permisos granulares en la consola de administración	
Debe permitir la creación de reportes programados y por demanda de las detecciones que se tienen	
Debe contar con un Dashboard permitiendo ver la información relevante de amenazas identificadas	
La solución debe acreditar capacidades de seguridad de correo mediante evaluaciones independientes, certificaciones reconocidas o informes técnicos verificables	
La solución deberá ofrecer mecanismos de autenticación de multiple factor (MFA) para usuarios administradores.	

3.1 OBLIGACIONES DEL CONTRATISTA:

3.1.1. OBLIGACIONES GENERALES:

1. Guardar la reserva debida tanto sobre el contenido de los documentos e información que, para la ejecución del objeto contratado le suministre LA ENTIDAD, si hay lugar a ello, así como del resultado de las mismas, salvo previa autorización expresa y escrita que reciba de aquella, reserva que es obligatoria también para las personas naturales y jurídicas que contrate bajo su responsabilidad.
2. Cumplir con sus obligaciones frente al Sistema de Seguridad Social Integral, Parafiscales (Cajas de Compensación Familiar, Sena e ICBF), y demás obligaciones a que haya lugar de acuerdo con la normatividad vigente al respecto. El incumplimiento de esta obligación será causal para que LA ENTIDAD inicie el procedimiento sancionatorio a que haya lugar.
3. Obrar con lealtad y buena fe, evitando dilaciones y entrabamientos.
4. No acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de obligarlo a hacer u omitir algún acto o hecho, informando inmediatamente a LA ENTIDAD y demás autoridades competentes cuando se presenten tales peticiones o amenazas.
5. Mantener actualizado su domicilio durante la vigencia del contrato.
6. Disponer lo necesario para que el objeto del contrato se cumpla a cabalidad.

7. Tener en cuenta las instrucciones de orden técnico y operativo que para el desarrollo del objeto del contrato disponga LA ENTIDAD.
8. Responder por la calidad del objeto contratado, de acuerdo con las previsiones de las normas vigentes aplicables a esta materia.
9. Informar oportunamente al supervisor del contrato cualquier discrepancia que encuentre referente a las especificaciones previstas.
10. Responder por todas aquellas obligaciones de la naturaleza del contrato que, pese a no estar escritas se consideren obligaciones a su cargo o estén contempladas en las reglamentaciones expedidas por el Gobierno Nacional.

3.1.2. OBLIGACIONES DEL CONTRATISTA FRENTE AL SISTEMA DE GESTIÓN AMBIENTAL:

EL CONTRATISTA debe dar cumplimiento a las disposiciones legales vigentes del SISTEMA DE GESTIÓN AMBIENTAL y en especial deberá:

a. Dar estricto cumplimiento a los lineamientos, normas, reglamentos, estándares, orientaciones, políticas, y leyes ambientales aplicables para la ejecución de las actividades contratadas por esta ENTIDAD.

b. Cumplir, sin excepción, la legislación ambiental vigente, sin necesidad de requerimiento previo o expreso; y obtener, mantener vigentes las licencias o permisos de autoridades ambientales que de conformidad con la normatividad vigente sean necesarias para cumplir sus obligaciones contractuales y/o post-contractuales, si a ello hubiere lugar.

PARÁGRAFO PRIMERO: Igualmente EL CONTRATISTA debe prever los costos en los que deben incurrir para el cumplimiento de las normas ambientales, antes, durante y después de la ejecución del contrato. **PARÁGRAFO SEGUNDO:** Las obligaciones ambientales que se consignan dentro del contrato se harán extensivas y serán de obligatorio cumplimiento por parte de los subcontratistas que hagan parte de la actividad que EL CONTRATISTA contractualmente desarrolla.

3.1.3. OBLIGACIONES DEL CONTRATISTA FRENTE AL SISTEMA DE SEGURIDAD Y SALUD EN EL TRABAJO:

El contratista, sin perjuicio de la obligación de cumplir con las disposiciones legales asociadas con la gestión de seguridad y salud en el trabajo, debe acatar las disposiciones que le fije el DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA – DAPRE, en especial las siguientes:

A. Suministrar al personal que se encuentre a su cargo y que dispondrá para la ejecución del contrato, todos los elementos de protección personal necesarios para desarrollar la actividad contratada, para lo cual asumirá su costo, si a ello hubiere lugar.

B. El personal de EL CONTRATISTA que se encuentre a su cargo y que dispondrá para la ejecución del contrato, deberá contar con todos los permisos y certificaciones necesarias para el desarrollo de la actividad o actividades requeridas, si a ello hubiere lugar.

C. Cumplir con las normas, reglamentos e instrucciones del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST.

3.1.4. OBLIGACIONES DEL CONTRATISTA RESPECTO DEL SISTEMA DE SEGURIDAD DE LA INFORMACION –SGSI:

El contratista deberá dar cumplimiento a las disposiciones legales vigentes del SISTEMA DE SEGURIDAD DE LA INFORMACION -SGSI y en especial deberá cumplir con los lineamientos, normas, reglamentos, estándares, orientaciones y políticas aplicables para la ejecución de las actividades contratadas por esta Entidad, tal como lo establece el Manual de Políticas de Seguridad de la Información M-TI-01.

3.1.5. OBLIGACIONES ESPECÍFICAS

- Renovar el licenciamiento de la solución integral de ciberseguridad para la totalidad de los activos definidos por la entidad, garantizando su vigencia y correcta activación, conforme a las especificaciones técnicas establecidas.
- Instalar, configurar, actualizar y garantizar la continuidad operativa de la solución tecnológica en la infraestructura de la Entidad, para asegurar su adecuado funcionamiento y el cumplimiento de las características técnicas exigidas.
- Garantizar la operación continua de la solución, incluyendo las actualizaciones necesarias del software, firmas y motores de detección, de acuerdo con las condiciones técnicas definidas.

- Prestar los servicios de soporte técnico y mantenimiento, atendiendo los incidentes dentro de los tiempos y condiciones establecidos por la entidad y realizando las gestiones necesarias para su solución.
- Cumplir con las políticas de seguridad de la información, los estándares aplicables y los lineamientos definidos por la entidad, garantizando la protección de la información y la adecuada gestión de incidentes.
- Contar con las certificaciones, respaldo del fabricante y capacidades técnicas exigidas, asegurando que los servicios prestados cumplen con las condiciones establecidas en las especificaciones técnicas.
- Disponer del personal requerido con la formación, experiencia y certificaciones exigidas para la correcta ejecución del contrato.
- Atender los requerimientos de la supervisión, suministrar la información que le sea solicitada y permitir el seguimiento y control de la ejecución contractual.
- Ejecutar todas las actividades necesarias para el cumplimiento del objeto contractual, conforme a las especificaciones técnicas, asumiendo los riesgos a su cargo y garantizando la correcta prestación del servicio durante la vigencia del contrato

4. CÓDIGO DEL CLASIFICADOR DE BIENES Y SERVICIOS DE LAS NACIONES UNIDAS - UNSPSC.

De acuerdo con la codificación de Bienes y Servicios del Código Estándar de Productos y Servicios de Naciones Unidas, el bien, obra o servicio se encuentra codificado de la siguiente manera:

SEGMENTO	FAMILIA	CLASE
43	4323	432328
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de administración de redes
43	4323	432332
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
43	4323	432327

SEGMENTO	FAMILIA	CLASE
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de aplicaciones de red
43	4323	432330
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de entorno operativo

Fuente: https://www.colombiacompra.gov.co/clasificador-de-bienes-y-Servicios

5. IDENTIFICACIÓN DEL CONTRATO A CELEBRAR:

Como resultado de la presente selección, se celebrará un contrato de un contrato de uso de licencia y prestación de servicios de soporte técnico, cuyo objeto consiste en la renovación del licenciamiento y del servicio de soporte de la solución tecnológica, para atender las necesidades que se enuncian en la descripción, justificación de la necesidad y del objeto del presente proceso.

6. MODALIDAD DE SELECCIÓN Y SU JUSTIFICACIÓN:

Dada la naturaleza del objeto a contratar y teniendo en cuenta que los bienes y servicios que se necesitan adquirir son de características técnicas uniformes y de común utilización, la modalidad de selección del presente proceso será la de Selección Abreviada por Subasta Inversa prevista en el literal a), numeral 2 del artículo 2º de la Ley 1150 de 2007.

El contrato resultante del proceso de Selección Abreviada por Subasta Inversa, se regirá por lo prescrito en las Leyes 80 de 1993 y 1150 de 2007 y su Decreto Reglamentario 1082 de 2015 y demás normas que adicionen, modifiquen o reglamenten la materia.

En cumplimiento de lo dispuesto en el Decreto 310 de 2021, que reglamenta el artículo 41 de la Ley 1955 de 2019 en relación con la obligatoriedad del uso de los Acuerdos Marco de Precios, la Entidad efectuó la verificación de los Acuerdos Marco de Precios (AMP) e Instrumentos de Agregación de Demanda (IAD) disponibles en la Tienda Virtual del Estado Colombiano (TVEC), con el propósito de establecer la existencia de mecanismos que permitieran satisfacer la necesidad objeto de la presente contratación.

Como resultado de dicha revisión, se constató que actualmente no existe un Acuerdo Marco de Precios ni un Instrumento de Agregación de Demanda vigente que permita atender integralmente los requerimientos funcionales, técnicos y operativos asociados a la adquisición de la solución de ciberseguridad requerida por la Entidad.

Particularmente, se verificaron los instrumentos vigentes relacionados con la adquisición de software, encontrando que el Instrumento de Agregación de Demanda denominado "Software por Catálogo II", con vigencia comprendida entre el 22 de noviembre de 2024 y el 21 de noviembre de 2027, excluye expresamente las soluciones de ciberseguridad de su alcance. En efecto, la respectiva Guía de Compra dispone que:

> *"El instrumento no pretende proporcionar un entorno para la venta de proyectos de desarrollo, consultorías, hosting, BPO, mantenimiento físico de equipos, ni soluciones de ciberseguridad, razón por la cual este tipo de productos y servicios no están disponibles".*

En consecuencia, dicho instrumento no constituye un mecanismo idóneo para satisfacer la necesidad que sustenta el presente proceso contractual.

De igual forma, se verificó la existencia de procesos orientados a la conformación de Acuerdos Marco de Precios para bienes y servicios de ciberseguridad, evidenciándose que la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente adelanta el proceso CCENEG-094-1-2026, destinado a la estructuración del primer Acuerdo Marco de Precios para este sector. No obstante, dicho proceso no se encuentra vigente a la fecha, razón por la cual no existe actualmente un acuerdo disponible que pueda ser utilizado por la Entidad para atender la necesidad identificada.

Por lo anterior, y considerando la inexistencia de un Acuerdo Marco de Precios o Instrumento de Agregación de Demanda aplicable al objeto contractual, la Entidad concluye que resulta procedente adelantar el presente proceso mediante la modalidad de selección abreviada por subasta inversa, de conformidad con lo previsto en la Ley 1150 de 2007, el Decreto 1082 de 2015 y las demás disposiciones que regulan la adquisición de bienes y servicios de características técnicas uniformes.

De otra parte, en cumplimiento de lo establecido en el artículo 2.2.1.2.1.2.12 del Decreto 1082 de 2015, se efectuó el análisis para evaluar la conveniencia de acudir al mecanismo de la Bolsa de Productos, determinándose que, si bien el objeto contractual presenta características de estandarización, también exige especificaciones técnicas particulares y

condiciones de ejecución que no se ajustan plenamente a la dinámica propia de negociación de dicho mecanismo, pues la eventual utilización de la Bolsa de Productos implicaría la asunción de costos adicionales, tales como las comisiones del comisionista, costos de estructuración del proceso y constitución de garantías, los cuales no representan una ventaja económica frente a la modalidad de subasta inversa, ni contribuyen de manera significativa a la optimización de los recursos públicos.

En este contexto, desde el punto de vista de oportunidad, eficiencia y economía, la modalidad de Selección Abreviada por Subasta Inversa permite garantizar de manera adecuada los principios de la contratación estatal, en particular los de transparencia, economía y selección objetiva, al propiciar un escenario de competencia efectiva que posibilita la obtención del mejor precio para la Entidad.

En consecuencia, se concluye que la modalidad seleccionada resulta idónea, eficiente y acorde con la normatividad vigente, asegurando la adecuada satisfacción de la necesidad institucional.

7. VALOR ESTIMADO DEL PRESUPUESTO OFICIAL Y JUSTIFICACIÓN DEL MISMO:

7.1. ESTUDIO DE MERCADO

La Oficina de Tecnologías y Sistemas de Información realizó un evento de solicitud de información a proveedores a través de correo electrónico, con la siguiente información:

Fecha de envío de Solicitud de Cotización	30 de octubre de 2026
Fecha de cierre recibo de cotizaciones	02 de noviembre de 2026
Medio a través del cual se efectuó la invitación a cotizar	Correo electrónico
Nº Empresas Invitadas	4
Nº Cotizaciones Recibidas	4

En este sentido, con el numeral 4, artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, la Entidad ha estructurado el valor estimado del contrato mediante un análisis de precios de mercado, tomando como referencia las cotizaciones recibidas.

Con base en lo anterior, a continuación, se resumen las cotizaciones en líneas anteriores, así:

NOMBRE EMPRESA INVITADA	ENVIÓ COTIZACIÓN (SI / NO)	CUMPLE CONDICIONES TÉCNICAS (SI / NO)
IKUSI	SI	SI
NEMESIS	SI	SI
HEIMCORE	SI	SI
HTS CORP	SI	SI

A continuación, se presentan los resultados de las cotizaciones recibidas y el promedio aritmético obtenido para cada ítem:

DESCRIPCIÓN	NEMESIS	HTS	HEIMCORE	IKUSI	PROMEDIO (Precio Techo)
Endpoint Security Pro	$169.329.969	$ 174.966.900	$ 171.904.520	$ 178.996.113	**$173.799.375**
Endpoint Security Essentials	$293.505.280	$ 303.275.900	$ 298.000.210	$ 310.259.929	**$301.260.330**
Email and collaboration security Essentials	$216.366.071	$ 223.568.800	$ 219.686.285	$ 228.717.255	**$222.084.603**
XDR for Email (EmDR)	$21.636.607	$ 22.356.900	$ 38.080.735	$ 22.871.726	**$26.236.492**
Soporte Técnico 7x24x365,	$59.162.073	$ 35.700.000	$ 32.858.958	$ 48.485.468	**$44.051.625**

DESCRIPCIÓN	NEMESIS	HTS	HEIMCORE	IKUSI	PROMEDIO (Precio Techo)
cantidad ilimitada de incidentes por un (1) año + IVA					
TOTAL	$760.000.000	$759.868.500	$ 760.530.708	$ 789.330.491	$767.432.425
PROMEDIO					

Con fundamento en las cuatro (4) cotizaciones recibidas y una vez analizados los valores económicos presentados por los proveedores para la renovación del licenciamiento, implementación, configuración, soporte y actualización de la solución integral de ciberseguridad requerida por la Entidad, se efectuó la comparación económica de los valores ofertados para cada uno de los componentes que integran la solución.

Como resultado del análisis de mercado, y con el propósito de establecer valores de referencia que reflejen las condiciones económicas observadas en las cotizaciones recibidas, la Entidad adoptó como metodología para la determinación del presupuesto oficial el promedio aritmético de los valores cotizados para cada ítem, estableciendo precios techo para cada uno. En consecuencia, el promedio obtenido para cada componente se establece como su precio techo, de manera que la estructuración económica del proceso se encuentra discriminada por ítem y sustentada en la información suministrada por los cuatro (4) proveedores consultados.

La utilización del promedio aritmético permite considerar en igualdad de condiciones la totalidad de las cotizaciones válidas y comparables recibidas. Para su cálculo, se toman los valores cotizados para cada uno de los ítems que integran la solución, obteniendo un valor promedio individual que se adopta como precio techo para el respectivo ítem.

Esta metodología proporciona un criterio uniforme, objetivo y verificable para el tratamiento de la información económica obtenida mediante el estudio de mercado y guarda concordancia con los principios de planeación, economía, transparencia y selección objetiva que orientan la contratación estatal, toda vez que la estimación económica se soporta en información proveniente de los proveedores consultados y en una regla de cálculo aplicada de manera uniforme a las cotizaciones recibidas.

En consecuencia, el promedio aritmético determinado para cada ítem constituye una referencia económica sustentada en la información recopilada durante el estudio de mercado y permite establecer precios techo individualizados, reduciendo el riesgo de que la estimación económica dependa de valores extremos o de la cotización de un proveedor en particular. La sumatoria de dichos valores determina el presupuesto oficial estimado del proceso, proporcionando una base objetiva para la estructuración económica y el posterior proceso de selección.

En consecuencia, la sumatoria de los precios techo establecidos para cada uno de los ítems determina un presupuesto oficial estimado de **SETECIENTOS SESENTA Y SIETE MILLONES CUATROCIENTOS TREINTA Y DOS MIL CUATROCIENTOS VEINTICINCO PESOS M/CTE ($767.432.425)**, el cual constituye el valor máximo previsto por la Entidad para la ejecución del objeto contractual, incluidos los impuestos, tasas, contribuciones, costos directos e indirectos y demás gastos necesarios para la correcta ejecución del objeto contractual.

Rubro presupuestal: A-02-01-01-006-002

Funcionamiento: _X_ ó Inversión: ___

8. INDICACIÓN DE REQUISITOS HABILITANTES:

8.1. REQUISITOS HABILITANTES TÉCNICOS

8.2.1 EXPERIENCIA GENERAL:

Se tendrá como experiencia general mínima habilitante del proponente la certificación de contratos ejecutados y/o terminados por el proponente, que sumados tengan la siguiente equivalencia expresada en Salarios Mínimos Legales Mensuales Vigentes:

SMLMV	**438,31**

La experiencia general se acreditará y verificará directamente con el Registro Único de Proponentes (RUP).

Se verificará por parte de la Entidad que el o los contrato(s) ejecutado(s) se encuentra(n) identificado(s) *en el siguiente o siguientes o cualquiera de los códigos del Clasificador de Bienes y Servicios*, a nivel de clase, así:

SEGMENTO	FAMILIA	CLASE
43	4323	432328
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de administración de redes
43	4323	432332
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de seguridad y protección
43	4323	432327
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de aplicaciones de red
43	4323	432330
Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de entorno operativo

NOTA 1: En caso de que los contratos que acreditan la experiencia tengan algún tipo de multa o sanción, no serán tenidos en cuenta por parte de **LA ENTIDAD**.

NOTA 2: PARA PROPONENTES EXTRANJEROS QUE NO ESTÁN OBLIGADOS A INSCRIBIRSE EN EL RUP: Para acreditar la experiencia a la que se refiere el presente numeral, el oferente extranjero que no está obligado a tener RUP debe presentar certificación suscrita por su representante legal anexando los documentos soporte (contrato y acta de liquidación o contrato y certificación de recibo a satisfacción), de conformidad con el anexo del pliego de condiciones.

NOTA 3: En caso de consorcio o unión temporal será válida la acreditación de la experiencia general por uno de sus miembros o en conjunto por sus integrantes, independientemente de su porcentaje de participación.

NOTA 4: Si la constitución del proponente es menor a tres (3) años, podrá acreditar la experiencia general de sus accionistas, socios o constituyentes, para lo cual deberá suscribir y aportar debidamente diligenciado el Anexo del pliego de condiciones, información que verificará la Entidad en el RUP aportado.

El proponente deberá acreditar experiencia específica con el aporte de máximo dos (02) certificaciones de contratos terminados y/o liquidados, cuyo objeto incluya el suministro, renovación, implementación, administración o soporte de plataformas de soluciones de protección de endpoints, antivirus, antimalware, EDR, XDR, prevención de pérdida de datos (DLP), seguridad de correo electrónico y/o soluciones integrales de ciberseguridad.

Para tal efecto, deberá acreditar:

- **Mínimo un (1) contrato ejecutado** cuyo objeto se encuentre directamente relacionado con el suministro, implementación, soporte o administración de soluciones de seguridad.
- Que el (los) contrato(s) acreditado(s) haya incluido la implementación, operación o gestión de funcionalidades de protección, monitoreo, detección y respuesta ante amenazas, administradas desde una consola o plataforma centralizada.

De conformidad con la naturaleza, objeto y características del presente proceso se considerará la experiencia acreditada, mediante la presentación de las siguientes certificaciones, teniendo en cuenta los criterios diferenciales para Mipymes, de conformidad con lo dispuesto en el Decreto 1082 de 2015, adicionado por el Decreto 1860 de 2021, así:

- **Para proponentes MIPYMES (Criterio Habilitante Diferencial):** Máximo tres (3) contratos terminados y/o liquidados por el proponente.
- **Para Proponentes diferentes a MIPYMES:** Máximo dos (02) contratos terminados y/o liquidados por el proponente.

La experiencia general se acreditará y verificará directamente con el Registro Único de Proponentes (RUP).

En todo caso, para verificar la información que no se encuentra discriminada en el RUP, se podrá presentar certificación (es) o acta de liquidación debidamente suscrita (s) por el contratante, que acredite el cumplimiento del proponente en un contrato celebrado con entidad pública o privada, que se encuentre TERMINADO Y/O LIQUIDADO y que cumpla los siguientes requisitos:

- Que sea expedida por quien tenga la facultad para hacerlo.
- Que la (sumatoria de las) certificación (es) o acta (s) de liquidación aportada (s), presente una cuantía de por lo menos el 100 % del Presupuesto Oficial establecido para el presente proceso, expresado en SMLMV.
- Que contenga un objeto similar o igual, es decir, suministro, renovación, implementación, administración o soporte de plataformas de soluciones de protección de endpoints, antivirus, antimalware, EDR, XDR, prevención de pérdida de datos (DLP), seguridad de correo electrónico y/o soluciones integrales de ciberseguridad
- En caso de que la certificación o acta de liquidación describan adición a un contrato principal, esta se verificará en conjunto con el contrato principal que está adicionando.
- Si la certificación o acta de liquidación viene liquidada en moneda diferente al peso, la Entidad procederá a su convertibilidad a pesos colombianos ($), tomando como base la TRM (tasa representativa del mercado) reportada por el Banco de la República a la fecha de terminación del respectivo contrato.

En las certificaciones deberá especificarse lo siguiente:

- Número del contrato, cuando a ello hubiere lugar.
- Contratante.
- El objeto.
- El valor o cuantía.
- Fecha de inicio.
- Fecha de terminación.
- En el evento de identificarse en las certificaciones o actas de liquidación aportadas, calificación desfavorable al contratista o que la prestación del servicio o entrega de los bienes a satisfacción, o notas similares; las mismas no serán tenidas en cuenta por la Entidad.

En el evento de que la certificación o acta de liquidación sea expedida por personas de derecho privado, el contratista deberá anexar a la misma: copia del contrato o su documento equivalente, en donde se puedan verificar su objeto, plazo y valor.

NOTA 1: En ningún caso se considerará la experiencia del contrato que se reporte vigente a la fecha de cierre del proceso de selección.

NOTA 2: En caso de presentarse más de las certificaciones requeridas o actas de liquidación, la Entidad hará la verificación correspondiente sobre la(s) de mayor valor.

NOTA 3: La certificación debe corresponder a un contrato certificado, sin embargo, se aceptará la acreditación de la experiencia requerida en una (1) certificación o actas de liquidación, siempre y cuando esta única certificación o liquidación del contrato cumpla con los requisitos establecidos en el presente numeral.

NOTA 4: El Departamento Administrativo de la Presidencia de la República se reserva el derecho de verificar la información consignada en la certificación o actas de liquidación.

NOTA 5: En el evento de propuestas presentadas por unión temporal o consorcio, la experiencia podrá corresponder a cualquiera de sus integrantes, de manera individual o conjunta, independientemente de su grado de participación, cumpliendo con los requisitos establecidos en el presente numeral.

NOTA 6:

6.1. Cuando el oferente presente certificación de experiencia o actas de liquidación en la cual conste que participó en la ejecución de un contrato bajo la modalidad de consorcio o unión temporal, esta deberá expresar su porcentaje de participación, con el fin de verificar el cumplimiento de los requisitos de cuantía y período de ejecución previstos en este numeral.

6.2. Para acreditar la experiencia solo se tendrá en cuenta el grado de participación que haya tenido el proponente en el consorcio o unión temporal; en tales eventos, se recuerda, la certificación o actas de liquidación debe contener exactamente el grado de participación.

NOTA 7: No se aceptan auto-certificaciones, ni certificaciones expedidas por miembros de consorcios o uniones temporales.

8.2.2 CERTIFICADO PARTNER AUTORIZADO

El oferente deberá acreditar y demostrar que se encuentra autorizado por el fabricante de la solución ofertada para su comercialización, renovación, implementación y soporte.

Para acreditar el cumplimiento de este requisito, el oferente deberá aportar certificación vigente expedida directamente por el fabricante, a nombre del proponente y con una antelación no mayor a treinta (30) días calendario respecto de la fecha de cierre del proceso, en la cual se indique que cuenta con un nivel de membresía a nivel Skilled, Expert o Élite,

o su denominación equivalente vigente dentro del programa de canales del fabricante, que garantice el respaldo para la comercialización, renovación y soporte de la solución ofertada.

La certificación deberá encontrarse vigente a la fecha de presentación de la oferta. Si el documento se encuentra en un idioma diferente al castellano, deberá acompañarse de la correspondiente traducción oficial al castellano.

En caso de propuestas presentadas mediante Consorcio o Unión Temporal, este requisito podrá ser acreditado por al menos uno (1) de sus integrantes.

8.2.3.DOCUMENTO DE COMPROMISO DE ACTUALIZACIÓN TECNOLÓGICA

Se deberá aportar documento emitido por el proponente o su representante legal, donde manifieste que: En caso de presentarse una actualización tecnológica en el software que forme parte de la solución propuesta, con anterioridad a la entrega definitiva, entregará tales elementos actualizados, contando con autorización del supervisor del contrato y sin que la Entidad incurra en costo adicional alguno.

Se entiende que hay una actualización tecnológica en cualquiera de los elementos ofrecidos, cuando se presenta una nueva versión en el mercado. En cualquier caso, el proponente no podrá ofrecer programas que estén descontinuados por el fabricante original.

8.2.4.CERTIFICACIÓN DE GARANTÍA

El proponente debe adjuntar una certificación de garantía vigente, es decir, con menos de 30 días de expedición a la fecha de cierre del proceso, lo cual se entenderá con que en la misma se haga referencia al presente proceso de selección, suscrita directamente por el fabricante, en la cual conste que otorgará garantía de la solución tecnológica durante el término de un (1) año, contado a partir de la entrega de la renovación del licenciamiento.

Si la misma se encuentra en un idioma diferente al español, deberá anexarse la traducción correspondiente al castellano. En caso de una Unión Temporal o un Consorcio, uno de los integrantes deberá acreditar la presente certificación

8.2. INDICADORES FINANCIEROS:

Para verificar la Capacidad Financiera y la Capacidad Organizacional, la Entidad tendrá en cuenta la información registrada en el Registro Único de Proponentes – RUP, la cual debe estar vigente y en firme.

NOTA 1: Cuando el proponente cuente con menos de un año de constituido, la entidad tendrá en cuenta la información registrada en el Registro Único de Proponentes – RUP del Balance de Apertura.

NOTA 2: En caso de consorcios o uniones temporales, los indicadores financieros (capacidad financiera y organizacional) se calcularán sobre la sumatoria de las cifras financieras reportadas en el RUP de los integrantes del Consorcio o Unión Temporal, independientemente del porcentaje de participación de sus integrantes.

NOTA 3: La propuesta será aceptada siempre que al aplicar cada uno de los indicadores, su resultado cumpla la condición de aceptada.

NOTA 4: Todos los proponentes que demuestren interés en participar en el presente proceso de contratación deberán estar inscritos en el Registro Único de Proponentes con el fin de que la entidad realice la verificación de los requisitos habilitantes de carácter financiero de conformidad con lo establecido en el Decreto 1082 de 2015 y el artículo 6 de la Ley 1150 de 2007 modificado por el artículo 221 del Decreto Ley 019 de 2012.

NOTA 5: En caso de que los proponentes no cumplan con el tamaño patrimonial requerido de forma individual, se sugiere que estos puedan unirse mediante consorcios o uniones temporales, con el fin de acreditar conjuntamente los requisitos patrimoniales exigidos en el proceso.

NOTA 6: OFERENTES EXTRANJEROS: Las empresas extranjeras interesadas en participar en el presente proceso deben enviar los Estados Financieros con corte a 31 de diciembre de 2025, de conformidad con la legislación propia del país de origen, avalados con la firma de quien se encuentre en obligación de hacerlo de acuerdo con la normativa vigente del país de origen, en idioma español y debidamente apostillados, (respecto de la apostilla aplica el numeral 1.19 del presente documento de términos y condiciones adicionales), adicionalmente deben especificar la moneda en la cual están presentados; con la anterior

información LA ENTIDAD procederá a establecer el valor en pesos de acuerdo con la tasa de cambio establecida por el Banco de la República del año fiscal 2025, adjunto en la propuesta, con el fin de calcular los índices financieros requeridos por LA ENTIDAD. De igual manera deberá diligenciar el correspondiente Anexo del pliego de condiciones.

8.2.1. CAPACIDAD FINANCIERA:

INDICADOR	INDICE REQUERIDO
Liquidez	Mayor o igual a **1,4**
Endeudamiento	Menor o igual a **68%**
Razón de Cobertura de Intereses	Mayor o igual a 0/Indeterminado

Adicionalmente y de conformidad con las características del objeto a contratar y la naturaleza del presente proceso de selección, la Entidad verificará el Tamaño Patrimonial en la información financiera registrada en el RUP que se encuentre en firme, es decir el valor registrado en el patrimonio, así:

INDICADOR	VALOR REQUERIDO
Tamaño Patrimonial	Mayor o igual a $693 Millones

CRITERIO HABILITANTE DIFERENCIAL

A los oferentes que acrediten su condición de Mipyme, en los términos señalados en la normatividad vigente les serán aplicables los siguientes criterios diferenciales en lo referente a los requisitos mínimos habilitantes de Capacidad Financiera:

INDICADOR	VALOR REQUERIDO
Tamaño Patrimonial	Mayor o igual a $520 Millones

En cumplimiento del parágrafo 1 del artículo 2.2.1.2.4.2.15. y el parágrafo 2 del artículo 2.2.1.2.4.2.18. del Decreto 1082 de 2015, tratándose de proponentes plurales, los criterios diferenciales solo se aplicarán si por lo menos uno de los integrantes acredita que: 1) Pertenece a la categoría de Mipyme o de empresa y emprendimiento de mujeres y 2) Que tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

Los oferentes deben cumplir con los índices requeridos por la Entidad para determinar la capacidad financiera.

Los oferentes cuyos gastos de intereses sean cero (0), no podrán calcular el indicador de razón de cobertura de intereses. En este caso el oferente cumple el indicador, salvo que la utilidad operacional sea negativa, caso en el cual NO cumple con el indicador de cobertura de intereses.

NOTA: En caso de presentarse la propuesta a través de consorcio o unión temporal se tomarán las cifras registradas en el RUP, de la información financiera en firme, por cada uno de los integrantes del consorcio o la unión temporal y se sumarán las cifras, con el fin de calcular los índices específicos de este documento para la asociación. Aplica de igual manera para la capacidad organizacional.

Cuando, como resultado de éste cálculo se generen cifras con decimales, LA ENTIDAD procederá a efectuar la aproximación de éstos así: si el resultado obtenido es inferior o igual a 50 decimales se baja a la unidad anterior y si por el contrario el resultado obtenido es superior o igual a 51 decimales se sube a la unidad siguiente, ejemplo: en una operación que genere un valor de 20.50 el valor registrado será 20 y para un resultado de 20.51 el valor final será de 21.

- Para el caso de consorcios o uniones temporales, la liquidez se determina así:

$$IL = \frac{AC1+AC2+AC3+ \ldots}{PC1+PC2+PC3+ \ldots}$$

IL: Índice de Liquidez

AC: Activo Corriente de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

PC: Pasivo Corriente de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la formula anterior, la cifra resultante **deberá ser mayor o igual a 1,4**

- Para el caso de consorcios o uniones temporales, el endeudamiento se determina así:

IE= PT1+PT2+PT3...

AT1+AT2+AT3...

IE: Índice Endeudamiento

PT: Pasivo Total de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

AT: Activo Total de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, el porcentaje resultante deberá ser menor o igual al 68%.

- Para el caso de consorcios o uniones temporales, la razón de cobertura de intereses se determina así:

RCI = (UO1+UO2+UO3…)

(GI1+GI2+GI3…)

RCI: Razón de Cobertura de Intereses

UO: Utilidad Operacional de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

GI: Gastos de Intereses de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, la Razón de Cobertura deberá **ser mayor o igual a 0 veces o indeterminado.**

Para el caso de consorcios o uniones temporales, cuando la suma de los gastos de intereses sean cero (0), no podrán calcularse el indicador de razón de cobertura de intereses. En este caso el oferente cumple el indicador, salvo que el total de la utilidad operacional de los

integrantes de la unión temporal o consorcio sea negativo, caso en el cual NO cumple con el indicador de cobertura de intereses.

- Para el caso de consorcios o uniones temporales, el Tamaño del Patrimonio se determina así:

TP = TP1+TP2+TP3….

TP = Sumatoria del Tamaño Patrimonial de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, el proponente deberá contar con el siguiente tamaño patrimonial, así:

INDICADOR	VALOR REQUERIDO
Tamaño Patrimonial	Mayor o igual a $693 Millones

CRITERIO HABILITANTE DIFERENCIAL

En cumplimiento del parágrafo 1 del artículo 2.2.1.2.4.2.15. y el parágrafo 2 del artículo 2.2.1.2.4.2.18. del Decreto 1082 de 2015, tratándose de proponentes plurales, los criterios diferenciales solo se aplicarán si por lo menos uno de los integrantes acredita que: 1) Pertenece a la categoría de Mipyme o de empresa y emprendimiento de mujeres y 2) Que tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

INDICADOR	VALOR REQUERIDO
Tamaño Patrimonial	Mayor o igual a $520 millones

8.2.2. CAPACIDAD ORGANIZACIONAL

La verificación de la capacidad organizacional se efectuará con base en la capacidad registrada en el Registro Único de Proponentes, la cual deberá estar actualizada y en firme acorde con lo dispuesto en el numeral 2.2. Requisitos Habilitantes Financieros.

INDICADOR	INDICE REQUERIDO
Rentabilidad del patrimonio	Mayor o Igual a 1%
Rentabilidad del activo	Mayor o Igual a 1%

Los oferentes deben cumplir con los dos índices establecidos por la Entidad para verificar la capacidad organizacional.

En caso de consorcio o unión temporal, el DAPRE calculará el indicador de Rentabilidad del Patrimonio, así:

RP = (UO1+UO2+UO3…)

(P1+PT2+PT3…)

RP = Rentabilidad del Patrimonio

UO = Utilidad Operacional de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

P = Patrimonio de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, la rentabilidad del patrimonio requerida deberá ser mayor o igual a 1%.

En caso de consorcio o unión temporal, el DAPRE calculará el indicador de Rentabilidad del Activo, así:

RA = (UO1+UO2+UO3…)

(AT1+AT2+AT3…)

RA = Rentabilidad del Activo

UO = Utilidad Operacional de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

AT = Activo Total de cada uno de los asociados o consorciados que integran el consorcio o la unión temporal

Una vez aplicada la fórmula anterior, la rentabilidad del activo requerida deberá ser mayor o igual a 1%.

8.3. DOCUMENTOS HABILITANTES JURÍDICOS

Los interesados podrán participar como proponentes bajo alguna de las siguientes modalidades:

A. Individualmente como: a) personas naturales nacionales o extranjeras, b) personas jurídicas nacionales o extranjeras.
B. Conjuntamente, como proponentes plurales en cualquiera de las formas de asociación previstas en el artículo 7 de la Ley 80 de 1993.

Los proponentes deben:

A. Tener capacidad jurídica para la presentación de la oferta.
B. Tener capacidad jurídica para la celebración y ejecución del contrato.
C. No estar incursos en ninguna de las circunstancias de inhabilidad, incompatibilidad, conflicto de interés o prohibición para contratar previstas en la Constitución y en la Ley.
D. No estar reportados en el último Boletín de Responsables Fiscales vigente publicado por la Contraloría General de la República. Esta disposición aplica para el proponente e integrantes de un proponente plural con domicilio en Colombia. Tratándose de proponentes extranjeros sin domicilio o sin sucursal en Colombia, deben declarar que no son responsables fiscales por actividades ejercidas en Colombia en el pasado y que no tienen sanciones vigentes en Colombia que impliquen inhabilidad para contratar con el Estado.

La entidad consultará los antecedentes judiciales en línea en los registros de las bases de datos, al igual que el certificado de antecedentes disciplinarios conforme el artículo 1 de la Ley 1238 de 2008 y el Registro Nacional de Medidas Correctivas del Ministerio de Defensa Nacional – Policía Nacional, de acuerdo con lo dispuesto en el artículo 184 de la Ley 1801 de 2016 – Código Nacional de Seguridad y Convivencia Ciudadana.

Los documentos para verificar la capacidad jurídica de los oferentes, serán los establecidos en el documento de términos y condiciones adicionales.

9. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE:

Para la escogencia del ofrecimiento más favorable, el Departamento Administrativo de la Presidencia de la República tendrá como único criterio de selección **el menor precio, conforme el último lance válido realizado en la diligencia de Subasta Inversa Electrónica**.

Se realizarán a través de la plataforma del SECOP II y deberán reflejar un decremento de mínimo 2% respecto del menor precio (oferta inicial de precio o lance anterior), el cual debe corresponder al decremento total de la oferta.

NOTA: El valor respecto del cual se efectuará el decremento es sobre el menor valor total ofertado (inicial o en el desarrollo de la subasta).

10. FORMA DE PAGO DEL CONTRATO:

El valor total del contrato se pagará por parte de LA ENTIDAD a EL CONTRATISTA, en un único pago equivalente al 100% del valor del contrato.

Los pagos se harán previo cumplimiento de los siguientes requisitos: i. El recibo a satisfacción de la renovación de la solución tecnológica, expedido por el supervisor del contrato, que garantice la prestación del soporte técnico por el término de la renovación. ii. Certificación expedida por el Contratista, Representante Legal o su Revisor Fiscal, cuando corresponda, donde se acredite estar a Paz y Salvo por concepto de pago de sus obligaciones a los Sistemas de Salud, Riesgos Laborales, Pensiones y Aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, de todo el personal a su cargo que así lo requiera según la norma a aplicable. de ingreso al Almacén de LA ENTIDAD iii. Ingreso a la bodega virtual de software, cuando ello aplique según la naturaleza de los bienes y servicios entregados. iv. Trámite de la cuenta respectiva.

El valor del contrato se cancelará a través de la pagaduría de la Entidad, contra facturación presentada por parte del contratista, con base en la entrega efectiva de la renovación del licenciamiento; el pago se realizará previo cumplimiento de los siguientes requisitos:

a) Aprobación por parte de la Entidad de la Garantía Única.
b) Certificación expedida por el Contratista o su Revisor Fiscal o Representante Legal, cuando corresponda, donde se acredite estar a Paz y Salvo por conceptos de pago de sus obligaciones a los sistemas de salud, riesgos laborales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, de todo el personal a su cargo que así lo requiera, la cual deberá acompañarse de la copia de la cédula, tarjeta profesional y certificado vigente de la Junta Central de Contadores, para el caso de los revisores fiscales.
c) Ingreso a la bodega virtual de software, previa validación de la certificación de garantía vigente.
d) Certificación emitida por parte del supervisor del contrato, en la cual se acredite la entrega y recibo a satisfacción de las licencias.
e) Trámite de la respectiva cuenta por parte de la Entidad.

NOTA 1. La Entidad pagará al **CONTRATISTA**, dentro de los diez (10) días hábiles siguientes a la radicación de los documentos del contrato en el Área Financiera de la Entidad.

NOTA 2. No obstante la forma de pago prevista, esta queda sujeta a la situación de los recursos por parte del Ministerio de Hacienda y Crédito Público una vez se encuentre aprobado el PAC (Programa Anual Mensualizado de Caja).

NOTA 3. Si la factura no ha sido correctamente elaborada o no acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para este solo empezará a contarse desde la fecha en que aporte el último de los documentos y/o se presenten en debida forma. Las demoras que se presenten por estos conceptos, serán responsabilidad de contratista y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza.

NOTA 4: Cuando a ello hubiere lugar, presentar como requisito necesario para el pago, la factura electrónica validada previamente por la DIAN conforme la Directiva Presidencial No. 09 del 17 de septiembre de 2020 y la Resolución No. 042 del 05 de mayo de 2020, modificada parcialmente por la Resolución No. 094 del 30 de septiembre de 2020, y dar cumplimiento a lo establecido en la circular publicada en la página WEB de **LA ENTIDAD** https://dapre.presidencia.gov.co/normativa/normativa/CIR21-00000022-IDM.pdf.

NOTA 5: Al pago se le efectuarán los respectivos descuentos por impuestos de ley y las contribuciones respectivas.

NOTA 6: El procedimiento para el pago podrá modificarse de conformidad con el trámite de la factura electrónica en el SIIF Nación.

11. PLAZO DE EJECUCIÓN DEL CONTRATO A CELEBRAR:

El plazo de ejecución será hasta de un (1) año y quince (15) días, contado a partir de la aprobación de la garantía única que debe constituir el Contratista y previa expedición del correspondiente registro presupuestal.

El plazo para la entrega de la renovación será de quince (15) días, previa expedición del registro presupuestal y aprobación de la garantía única.

La renovación del licenciamiento tendrá una vigencia de un (01) año, contado a partir de la entrega de la misma, término en el cual se prestará el servicio de soporte técnico a que haya lugar.

12. LUGAR DE ENTREGA DE LOS BIENES O DE PRESTACIÓN DEL SERVICIO:

Para todos los efectos, se tendrá como lugar de ejecución del contrato la Ciudad de Bogotá D.C. en la Calle 7 # 6-54.

NOTA: Cuando se requiera que el servicio de soporte técnico en sitio, el mismo se realizará en la Ciudad de Bogotá D.C., en la Calle 7 # 6-54

13. LIQUIDACIÓN.

De conformidad con lo dispuesto por los artículos 60 de la Ley 80 de 1993, modificado por el artículo 217 del Decreto 019 de 2012, y el artículo 11 de la Ley 1150 de 2007, el contrato se debe liquidar dentro de los seis (6) meses siguientes a su terminación.

14. ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO:

Conforme lo establecido en el artículo 4 de la Ley 1150 de 2007 y en el numeral 6° del artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, debe existir un soporte que permita la tipificación, estimación y asignación de los riesgos previsibles.

Se entienden como riesgos involucrados en la contratación cualquier evento que puede generar efectos adversos y de distinta magnitud en el logro de los objetivos del Proceso de Contratación o en la ejecución de un contrato (artículo 2.2.1.1.1.3.1. del Decreto 1082 de 2015), así como todas aquellas circunstancias que, de presentarse durante el desarrollo y ejecución del contrato, tienen la potencialidad de alterar el equilibrio económico del mismo, pero que dada su previsibilidad se regulan en el marco de las condiciones inicialmente pactadas en los contratos y se excluyen así del concepto de imprevisibilidad de que trata el artículo 27 de la Ley 80 de 1993. LA ENTIDAD realizó el ejercicio de previsibilidad ordenado por las normas ya mencionadas el cual tuvo en consideración adicionalmente lo dispuesto en Documento CONPES sobre Riesgo Previsible en el Marco de la Política de Contratación Pública expedido por el Consejo Nacional de Política Económica y Social del Departamento Nacional de Planeación.

En el ejercicio de previsibilidad se analizaron aspectos tales como la naturaleza del contrato, el plazo de ejecución, las obligaciones a cargo del contratista, los bienes y/o servicios a contratar, así como los demás aspectos enunciados en el estudio del sector, entre otros.

Como resultado del ejercicio de previsibilidad, LA ENTIDAD determinó los siguientes riesgos partiendo de las características propias del contrato, así como las condiciones generales de objeto a contratar, el plazo, forma de pago, entre otros:

	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	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad
1	General	Interno	Contratación	Operacional	Incumplimiento en la verificación de los requisitos técnicos, funcionales, de licenciamiento, soporte, económicos y legales exigidos para la renovación de licencias de la solución integral de ciberseguridad y servicios asociados de soporte técnico	Selección de oferentes que no garantizan la correcta prestación del servicio. Adquisición de licencias no válidas o insuficientes. Investigaciones disciplinarias y posibles sanciones.	3 Posible	4. Mayor	6	Alto	Contratante - Contratista	Verificación exhaustiva de cumplimiento de requisitos habilitantes y técnicos, validación de licenciamiento oficial del fabricante y condiciones de soporte	1.Raro	1. Insignificante	2	Bajo	Sí	Comité evaluador	Etapa proceso contractual	Evaluación	Revisión Documental	Permanente en el Proceso Contractual
2	Específico	Externo	Planeación	Financiero	Variación de la TRM que afecte el costo de la renovación de licencias de la solución integral de ciberseguridad	Desequilibrio económico del contrato	3 Posible	3. Moderado	6	Alto	Contratista	Aceptar el Riesgo no puede ser evitado ni ser transferido o el costo de evitarlo o transferirlo es muy alto. En este caso se recomienda al contratista tomar medidas para reducir el Riesgo o mitigar su impacto, como son: Planeación financiera adecuada, cobertura cambiaria o previsión en la estructuración de la oferta.	3. Posible	2.Menor	5	Alto	Sí	Contratista	Etapa de ejecución si ocurre la situación	Pagos	Cumplimiento de las clausulas económicas y plan financiero	Revisión periódica o por facturación
3	General	externa	ejecución	regulatorio	Cambios en el régimen normativo o tributario que impacten la renovación y/o uso de licencias y la prestación del soporte técnico.	Desequilibrio de la ecuación contractual	3 Posible	2. Menor	5	medio	Contratista y entidad	Reducir las consecuencias a través de planes de contingencia	3. Posible	2.Insignificante	5	bajo	Sí	Contratista	Etapa de ejecución si ocurre la situación	Pagos	Cumplimiento de las clausulas económicas y plan financiero	Revisión periódica o por facturación
4	Específico	Externo	Ejecución	Operacional	El proveedor no cumple los tiempos de respuesta y solución del soporte técnico contratado.	Interrupciones en la protección. Afectación a la operación institucional.	3 Posible	3. Moderado	6	Alto	Contratista	Definición clara de SLA y penalidades. Seguimiento a tickets y tiempos de atención.	3. Posible	2.Insignificante	5	bajo	Sí	Contratista	Etapa de ejecución si ocurre la situación	Vencimiento Licencias	Reportes de mesa de servicio	Mensual.

	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	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad
4	Específico	Externo	Ejecución	Operacional	Las firmas, motores o versiones de la solución integral de ciberseguridad no se actualizan oportunamente.	Vulnerabilidad frente a nuevas amenazas. Incidentes de seguridad informática.	3 Posible	2. Menor	5	medio	Contratista	Exigir actualizaciones automáticas incluidas en el licenciamiento. Monitoreo del estado de actualización.	3. Posible	2.Insignificant	5	bajo	Sí	Contratista	Etapa de ejecución si ocurre la situación	Vencimiento Licencias	Consola central de administración.	Continua.

Por lo anterior el proponente que resulte adjudicatario del contrato, tendrá la absoluta responsabilidad en la ejecución de todas las actividades necesarias para la total y cabal ejecución del objeto y debe considerar todos los aspectos técnicos, económicos, financieros, y del mercado para evitar la ocurrencia de situaciones y materialización de riesgos que afecten la cabal ejecución del contrato y la permanencia de la ecuación contractual durante toda la vigencia del contrato, y en tal evento, serán de su cargo y responsabilidad los gastos que esto conlleve.

Ahora bien, conforme a lo dispuesto por el Documento CONPES sobre Riesgo Previsible en el Marco de la Política de Contratación Pública en el cual se advierte que:

"(…) será posible en las demás modalidades de selección recibir las observaciones que sobre el particular deseen formular los interesados tanto en la publicación del proyecto de pliego y pliego definitivo, como en las aclaraciones a los mismos pudiendo incluso citar a audiencia si se considera necesario. Lo anterior, en atención a su experticia en el objeto contractual y la gestión de los riesgos inmersos en él".

En consecuencia, los posibles oferentes o interesados en participar en el proceso deberán manifestar a LA ENTIDAD, a través del SECOP II, teniendo en cuenta el conocimiento que tienen como expertos en su actividad ordinaria, la existencia de posibles riesgos asociados a la ejecución del contrato que puedan afectar el cumplimiento del objeto contractual, en consecuencia, LA ENTIDAD no aceptará reclamaciones relacionadas con circunstancias

previsibles por el contratista que afecten el cumplimiento del contrato y que no hayan sido manifestadas por el mismo, en tal plazo.

14.1 RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

Adicional a lo anterior, LA ENTIDAD ha contemplado los siguientes riesgos de seguridad y privacidad de la información que se pueden presentar durante el desarrollo del Contrato, como son: pérdida la confidencialidad, integridad, disponibilidad y privacidad de los datos, los cuales podrían ocasionar que se interrumpa la prestación de los servicios.

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
1	Posibilidad de afectación reputacional, por la pérdida de disponibilidad de los servicios TICs, debido a la falta de seguimiento y monitoreo de las herramientas TICs - SGSI	Corresponde a los servicios que hacen parte de la Oficina de Tecnologías y Sistemas de Información, que puedan estar no disponibles.	SGSI	Mala identificación de los requisitos técnicos y funcionales	Indisponibilidad de los servicios de TICs	Alta	Mayor	Aplicar el procedimiento de control de cambios
				Errores humanos	Violación a las políticas de seguridad			Implementar actualizaciones de las diferentes aplicaciones utilizadas en la Entidad
				No cumplimiento del procedimiento establecido	Pérdida de imagen			Monitorear los servicios tecnológicos
				Error en la manipulación de la Plataforma Tecnológica	Quejas, reclamos frente a la prestación de servicios			Realizar la entrega de Rol con las respectivas actividades
				Dualidad de tareas en los funcionarios				Ejecutar pruebas de los servicios tecnológicos replicados en el centro alterno
				No activación de registros de logs				
				Error en las configuraciones de los controles				
				Deficiencias en cultura de la seguridad de la información e Informática	Retrasos en los procesos de los funcionarios y contratistas			Utilizar la herramienta de prevención de perdida de información (DLP)
				Fallas Técnicas de Hardware	Problemas de Seguridad Nacional (perdida de Información reservada)			Emplear la Autenticación de dos factores
				Conflicto Armado	Afectación derechos a titulares de datos personales			Aplicar Cifrado de Información pública clasificada y pública reservada

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
2	Posibilidad de afectación reputacional, por la pérdida de la documentación pública reservada y publica clasificada, o identificable de carácter personal (datos personales) que se encuentra en la Plataforma de TI o repositorios físicos, debido a accesos no autorizados - SGSI	En caso de que se presente perdida de información pública reservada o pública clasificada, o de carácter privado (información identificable como personal - datos personales) puede ocasionar afectación en la imagen de la Entidad.	Tecnología	Vandalismo Informático	Sanciones legales y disciplinarias	Media	Mayo	Realizar la verificación de vulnerabilidades de la plataforma TICs
				Desconocimiento del manual de políticas de seguridad.	Afectación de la imagen de la Entidad			Mantener operativas las herramientas tecnológicas
				Usuarios inconformes que puedan atentar contra la seguridad de la información				Realizar la entrega de Rol con las respectivas actividades
				Falta de conocimiento técnico en el personal que administra la plataforma informática o la información.				Ejecutar los procedimientos de backup, configuración de SAN
				Gestión de vulnerabilidades de la plataforma				Monitorear las herramientas de seguridad de la información
				Errores Humanos				Aplicar Políticas de Seguridad de la información
				Ataques cibernéticos y delitos informáticos				Utilizar contraseñas seguras.
				Obsolescencia de la plataforma				
				Deficiencias en definición, aplicación o seguimiento de las políticas de seguridad				
				Dualidad de tareas en los funcionarios				
				Deficiencias en el procedimiento de Borrado Seguro				
				Pérdida de equipos tecnológicos con información contenida				
3	Posibilidad de afectación reputacional, por pérdida de la gestión de la	La Entidad puede ser afectada por no disponer de una gestión de la continuidad del negocio al no	SGSI	Fallas en los equipos tecnológicos	Afectación de la Imagen de la Entidad	baj	Myor	Realizar pruebas de disponibilidad y continuidad para los servicios que proporciona la Entidad.

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
	continuidad del negocio en activos de información, debido a situaciones adversas - SGSI	tener la prestación de sus servicios, por situaciones adversas.		Falta de Mantenimientos preventivos	Retrasos en los procesos de los funcionarios			Aplicar los cambios a los sistemas mediante el uso de procedimientos formales de control de cambios.
				Desconocimiento del manual de políticas de seguridad	Retrasos en los procesos de los contratistas			Actualizar la documentación para la continuidad de la seguridad de la información.
				Equipos desactualizados	Problemas de Seguridad Nacional (pérdida de Información reservada)			
					Pérdida de credibilidad de las herramientas informáticas			
					Sanciones legales y disciplinarias			
					Retrasos en los procesos de los funcionarios			
4	Posibilidad de afectación reputacional, por el uso indebido de la información pública clasificada y/o pública reservada de la Entidad, así como de aquella identificable de carácter personal (datos personales), debido a la falta de controles para la protección de la información -SGSI	La información activa o cuando ha dejado de utilizarse debe gestionarse de una forma segura, porque la información clasificada o reservada, así como aquella identificable de carácter personal (datos personales) contenida en medios digitales o físicos (hojas de papel, carpetas, folletos, dispositivos de almacenamiento - memoria USB, disco duro - , medios magnéticos y ópticos) puede ser manipulada o utilizada por delincuentes para aprovechar su contenido con	SGSI	Deficiencias en el procedimiento de Borrado Seguro	Retrasos en los procesos de los funcionarios y contratistas	media	catastrófico	Aplicar el procedimiento de borrado seguro para equipos.
				Pérdida de equipos tecnológicos con información contenida.	Problemas de Seguridad Nacional (perdida de Información reservada)			Realizar la eliminación de documentos de archivo de acuerdo al procedimiento establecido por la Entidad.
				Desconocimiento de Baja de Bienes	Afectación derechos a titulares de datos personales			Utilizar la criptografía para mantener protegida información
				Desconocimiento del manual de políticas de seguridad	Sanciones legales y disciplinarias			Proteger la información mediante políticas y procedimientos de la Seguridad de la Información

No.	Nombre del Riesgo	Descripción del Riesgo	Clase de riesgo	Causas	Efectos	Probabilidad	Impacto	Controles
		fines distintos a la finalidad de dicha información (sea organizacional o personal) y afectar la imagen de la Entidad.		Deficiencias en cultura de la seguridad de la información e Informática	Afectación de la imagen de la Entidad			
				Desconocimiento procedimiento de eliminación de Documentos				
5	Posibilidad de afectación reputacional, por hurto, perdida o fuga de información, debido a ataques cibernéticos - SGSI	Los ataques cibernéticos se pueden presentar en la Entidad ocasionados por personas malintencionadas (ciberatacantes), afectando sistemas de información, aplicativos informáticos, páginas Web, equipos de cómputo, servidores que contienen y procesan información, comprometiendo la Confidencialidad, Integridad y Disponibilidad de la información.	SGSI	Ataques cibernéticos y delitos informáticos	Afectación de la Imagen de la Entidad	Muy Alta	Catastrófico	Gestionar las vulnerabilidades técnicas
				Falta de conocimiento técnico en el personal que administra la plataforma informática	Retrasos en los procesos de los funcionarios			Aplicar la seguridad de servicios de las aplicaciones en redes públicas.
				Falta de Verificación de vulnerabilidades de la plataforma TIC	Retrasos en los procesos de los contratistas			Proteger los activos de información contra los códigos maliciosos
				Obsolescencia de la plataforma	Problemas de Seguridad Nacional (pérdida de Información reservada)			Realizar la separación de redes
				Desconocimiento Manual de políticas de Seguridad de la Información	Pérdida de credibilidad de las herramientas informáticas			Utilizar Perímetros de Seguridad Física
					Sanciones legales y disciplinarias			Restringir el acceso a código fuente de Programas evitar cambios involuntarios.
								Utilizar contraseñas seguras
								Revisar la configuración y afinamiento de las herramientas de seguridad informática.
								Contener el Ataque Cibernético

15. PROYECTOS DE INVERSIÓN:

Señale si esta contratación es financiada con recursos de Proyectos de Inversión SI (__) NO (X)

NOMBRE PROYECTO DE INVERSIÓN	N/A
CÓDIGO BPIN	N/A
OBJETIVO (S) ESPECÍFICO (S)	N/A
PRODUCTO (S)	N/A
ACTIVIDAD (ES)	N/A
INDICADOR (ES)	N/A
BREVE DESCRIPCIÓN DE CÓMO CONTRIBUYE ÉSTA CONTRATACIÓN AL CUMPLIMIENTO DEL PROYECTO DE INVERSIÓN	N/A

Conforme lo anterior, se certifica que el presente proceso de selección se encuentra alineado con el proyecto de inversión respectivo.

16. GARANTÍAS

16.1 GARANTÍA DE SERIEDAD DE LA OFERTA

El proponente acompañará con su propuesta una garantía de seriedad, mediante cualquiera de los mecanismos vigentes previstos en el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015.

La garantía será expedida y cumplirá los requisitos establecidos para cada instrumento en el Decreto 1082 de 2015:

BENEFICIARIO: La Nación y/o Departamento Administrativo de la Presidencia de la República.
(NIT. 899999083-0)

AFIANZADO: El Oferente

VIGENCIA: Tres (03) meses, contados a partir de la presentación de la propuesta. En todo caso, su vigencia deberá extenderse hasta la aprobación de la garantía que ampara los riesgos propios de la etapa contractual

CUANTÍA: Diez por ciento (10%) del valor del presupuesto oficial.

16.2 OTRAS GARANTÍAS

16.2.1 GARANTÍA ÚNICA DE CUMPLIMIENTO:

Para avalar el cumplimiento idóneo y oportuno de las obligaciones estipuladas, el pago de las multas, de la pena pecuniaria y demás sanciones que, dado el caso, pudieren imponerse, **EL CONTRATISTA** deberá prestar una garantía única, consistente en póliza expedida por una compañía de seguros legalmente autorizada para funcionar en Colombia a favor de la **NACIÓN Y/O EL DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA,** (Nit: 899.999.083-0). Dicha garantía tiene por objeto.

AMPARO	VIGENCIA	MONTO ASEGURADO
Cumplimiento del contrato	Plazo de ejecución del contrato y **seis (6) meses más**.	20% del valor total de este contrato
Calidad y correcto funcionamiento de los bienes		
Calidad del servicio		
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	Plazo de ejecución del contrato y tres **(3) años más**.	5% del valor total de este contrato

16.2.2 **PÓLIZA DE RESPONSABILIDAD CIVIL EXTRACONTRACTUAL:**

VIGENCIA	VALOR ASEGURADO
Plazo de ejecución del contrato	200 salarios mínimos legales mensuales vigentes y con una vigencia igual al plazo de ejecución del contrato

16.2.3 OTRAS GARANTÍAS:

No se requieren otras garantías.

17. INDICACIÓN DE SI EL PROCESO DE CONTRATACIÓN ESTÁ COBIJADO POR UN ACUERDO COMERCIAL.

En cumplimiento de lo dispuesto en el numeral 10 del artículo 2.2.1.1.2.1.3 del Decreto 1082 de 2015 y en atención al Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación expedido por Colombia Compra Eficiente, para la presente contratación aplican los siguientes tratados de Libre Comercio:

Acuerdo Comercial		Vigente	Entidad Estatal incluida	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
Alianza Pacífico	Chile	SI	SI	SI	NO	SI
	México	SI	SI	SI	NO	SI
	Perú	SI	SI	SI	SI	NO
Canadá		SI	SI	SI	SI	NO
Chile		SI	SI	SI	SI	SI
Corea		SI	SI	SI	SI	NO
Costa Rica		SI	SI	SI	SI	NO
Estados Unidos		SI	SI	SI	SI	NO
Estados AELC		SI	SI	SI	SI	NO
México		SI	SI	SI	SI	NO
Triángulo Norte	El Salvador	SI	SI	N/A	SI	NO
	Guatemala	SI	SI	N/A	SI	NO
	Honduras	SI	NO	N/A	N/A	NO
Unión Europea		SI	SI	SI	SI	NO
Israel		SI	SI	SI	SI	NO
Reino Unido e Irlanda del Norte		SI	SI	SI	SI	NO
Comunidad Andina de Naciones		SI	N/A	N/A	SI	SI

18. SUPERVISIÓN

La coordinación, supervisión y control de ejecución del contrato derivado del presente proceso de selección la realizará la Entidad y se ejercerá a través del **Coordinador del Grupo de Ciberseguridad**, quien velará por los intereses del DAPRE y tendrá, además de las funciones que por la índole y naturaleza del contrato le sean propias, las establecidas en el Manual de Contratación y la Guía de Supervisión vigentes.

19. NECESIDAD DE CONTAR CON INTERVENTORÍA:

La presente contratación SI ___ NO_X_ requiere de interventoría.

20. OTRAS OBSERVACIONES:

Se anexan CDP, Formato de oferta económica, cotizaciones, Anexo técnico, correo recibido por parte del Área Financiera con los Indicadores Financieros del Proceso.

VIRGUES MORENO YULL FREDY

Firmado digitalmente por VIRGUES MORENO YULL FREDY
Fecha: 2026.11.18 11:02:42 -05'00'

YULL FREDY VIRGÜES MORENO
Jefe Oficina de Tecnologías y Sistemas de Información

Proyecto: Jeisson Garzón Castiblanco – Contratista - Oficina de Tecnologías y Sistemas de Información