MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE INTELIGENCIA POLICIAL
GRUPO INVESTIGACIÓN, INNOVACIÓN Y ANALÍTICA DE DATOS

GS- 2026 -016501 / DIPOL – GRIAN – 20.1

Bogotá D.C., 24 ABR 2026

Señor mayor
PEDRO DAVID MONDRAGÓN PIÑEROS
Jefe Grupo de Contratos
Avenida Boyacá 142 A 55
Bogotá D.C.

Asunto: consolidado evaluaciones comités proceso PN DIPOL SA 020-2026

Respetuosamente me permito remitir a mi mayor, el consolidado de las evaluaciones de los comités técnico, económico y jurídico de las ofertas presentadas por las firmas **HIGH TECH SERVICES CORP** y **REALTIME CONSULTING & SERVICES SAS** realizadas en el marco del proceso PN DIPOL SA 020-2026, cuyo objeto es el ***"ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL"***,

COMITÉ	HIGH TECH SERVICES CORP	REALTIME CONSULTING & SERVICES SAS
Técnico	NO CUMPLE	NO CUMPLE
Econónimo	NO CUMPLE	NO CUMPLE
Jurídico	NO CUMPLE	NO CUMPLE

Con base a lo anterior, es preciso indicar lo siguiente:

COMITÉ TÉCNICO: mediante comunicación oficial GS-2026-016481-DIPOL del 23/04/2026, presentó la siguiente respuesta:

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
1.	**GENERALES**				
1.1	La adquisición del licenciamiento para la solución tecnológica de protección de correo electrónico y herramientas de colaboración en la nube deberá permitir la conexión y gestión de 400 cuentas de correo.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
1.2	**MARCA:** la que indique el oferente **REFERENCIA:** la que indique el oferente **FABRICANTE:** la que indique el oferente		X	X Trend AI TREND VISION ONE	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
				Trend Micro Incorporated	
2.	PROTECCIÓN DE CORREO				
2.1	La solución deberá tener la capacidad para proteger correos internos de la organización que provengan de la plataforma de Microsoft Office 365		X	X	
2.2	La solución deberá tener la capacidad para proteger correos en la plataforma Microsoft Office 365 de dominio externos y ajenos a la empresa		X	X	
2.3	La solución deberá tener motores para la detección de malware con la capacidad de identificar Exploits en documentos y archivos de Office.		X	X	
2.4	La solución deberá tener Sandbox para análisis de amenazas desconocidas y ataques de día cero.		X	X	
2.5	La solución deberá ofrecer un análisis de riesgo para reducir el impacto en los usuarios		X	X	
2.6	La solución deberá tener escaneo de URL en el cuerpo de los correos y en los archivos adjuntos.		X		X
2.7	La solución deberá ofrecer protección avanzada contra amenazas para OneDrive, SharePoint, Teams.		X		X
2.8	La solución debe tener una capacidad de protección colaborativa para detectar archivos maliciosos que se encuentran en SharePoint, OneDrive, Teams.		X		X
2.9	La solución deberá tener plantillas personalizables de DLP para controlar la fuga de información permitiendo realizar pruebas de expresiones regulares y listados de palabras para nuevas plantillas		X		X
2.10	La solución deberá tener DLP a nivel de Email con la capacidad de descubrir y reportar violaciones a las políticas.		X		X
2.11	La solución deberá tener DLP a nivel de SharePoint, Teams y One Drive, con la capacidad de descubrir y reportar violaciones a las políticas.		X		X
2.12	La solución deberá ofrecer disponibilidad del servicio superior a >99%.		X		X
2.13	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 (Limpiar, Eliminar, Tag, encriptar, notificar).		X		X
2.14	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.		X		X
2.15	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.		X		X
2.16	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 dé clic en el enlace		X		X
2.17	La solución deberá tener la capacidad en la consola en la nube de reportar ataques dirigidos.		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
2.18	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.		X	X	
2.19	La solución debe proporcionar seguridad para la información que se encuentra almacenada en la nube y garantizar la privacidad de la misma.		X		X
2.20	La solución debe tener la capacidad de identificar amenazas que aún no han sido reportadas con el análisis de los archivos.		X	X	
2.21	La solución debe proporcionar protección contra ataques de BEC (Business Email Compromise – Compromiso en cuentas corporativas) con el análisis de los mensajes.		X	X	
2.22	La solución debe contar con la capacidad de detectar el análisis de estilo de escritura impulsado por la IA embebida en la solución de los usuarios de alto perfil para detectar ataques BEC		X	X	
2.23	La solución debe contar con la capacidad de tener una funcionalidad de inteligencia correlacionada		X	X	
2.24	La solución debe contar con la capacidad de detectar posando el mouse en las url's adjuntas al correo, según a nivel reputacional y bloquear el acceso a determinado sitio web, cuando el mismo infrinja la reputación		X	X	
2.25	La solución debe tener la capacidad de detectar ataques dirigidos mediante explotación de archivos.		X	X	
2.26	La solución debe tener la capacidad de realizar un análisis avanzado de los archivos usando Machine Learning, para identificar amenazas que aún no han sido reportadas, pero que pueden generar una afectación sobre los datos o el sistema que está utilizando el usuario.		X	X	
2.27	La solución debe tener la capacidad de brindar protección contra ataques avanzados como Business Email Compromise (BEC), Ramsomware, Phishing avanzado entre otros ya sea mediante firmas anti-spam o reglas heurísticas.		X	X	
2.28	La solución debe tener la capacidad de tomar una acción 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.		X		X
2.29	La solución debe tener la capacidad de tomar una acción 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.		X		X
2.30	La solución debe tener la capacidad de tomar una acción sobre los archivos localizados en el servicio Sharepoint, Teams, One Drive y que sean analizados con el sandbox e identificados como maliciosos o sospechosos, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una descripción en el correo para informar al usuario por que el correo ha sido enviado a cuarentena o eliminados.		X	X	
2.31	La solución debe tener la capacidad de notificar al usuario cuando algún correo que iba dirigido a tuvo alguna acción reactiva, basado en las reglas configuradas, dicha notificación debe indicarle que acción se tomó sobre el		X		X

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	correo que iba dirigido a él y la razón de esta.				
2.32	La solución debe tener la capacidad de sincronizarse y actualizar la lista de objetos sospechosos cuando se existe la integración con la consola de gestión.		X		X
2.33	La solución debe tener la capacidad de integrarse con el Active Directory Federation Services o Microsoft Azure AD, para permitir agregar usuarios administradores locales que puedan administrar la consola usando las credenciales registradas en estos servicios		X	X	
2.34	La solución debe contar con la capacidad de tener una funcionalidad para gestionar integraciones de tecnologías de terceros como Firewalls Fortinet, Palo Alto, SIEM Qradar y Directorio Activo On-Premise y opcionalmente con Gestores de vulnerabilidades, Proveedores de nube, Dominios, para enviar información hacia las determinadas fuentes o en algunos casos, recibir información de estas para alimentar la postura de riesgo de la compañía.		X	X	
2.35	La solución debe permitir a los administradores configurar la lista de excepciones, de los archivos detectados mediante Machine Learning como maliciosos o sospechosos.		X		X
2.36	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 prevención de filtración de datos de la organización.		X	X	
2.37	La solución debe permitir realizar un escaneo manual en modo de evaluación para permitir a los administradores verificar las reglas que serán aplicadas para proteger Office 365 sin tomar ninguna acción sobre dichos correos o archivos.		X	X	
2.38	La solución debe tener una tecnología de reputación web para escanear URL en mensajes de correo electrónico y rastrear la credibilidad de los dominios web asignando un puntaje de reputación basado en factores que incluyen la antigüedad del sitio web, cambios históricos de ubicación e indicaciones de actividades sospechosas descubiertas a través del análisis del comportamiento de malware, como ataques de phishing que están diseñados para engañar a los usuarios para que proporcionen información personal.		X	X	
2.39	La solución debe soportar la extracción de URL de códigos QR para detener ataques de phishing, ransomware y BEC.		X	X	
2.40	La solución debe soportar el escaneo dinámico de URL y rastrear las páginas web de URL no probadas en tiempo real para determinar si las páginas contienen patrones maliciosos para proteger a los usuarios de ataques de phishing de día cero.		X	X	
2.41	La solución debe aprovechar la visión computacional basada en inteligencia artificial (IA) para analizar elementos de sitios web de marca y reconocer sitios falsos para proteger a los usuarios contra el phishing de credenciales.		X	X	
2.42	La visión artificial basada en IA debe poder reconocer elementos clave de una página o formularios de inicio de sesión de un servicio en la nube válidos para ayudar a evitar que los usuarios envíen credenciales a sitios no confiables y ayudarlos a deshacerse de la vulneración de la cuenta.		X		X

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
2.43	La solución debe ofrecer capacidad de prevención de pérdida de datos (DLP) tanto para mensajes de correo electrónico como para archivos en servicios de colaboración en la nube.		X	X	
2.44	La solución debe ofrecer la correlación de datos de correo electrónico XDR entre capas o más allá con identidad, punto final, red y otros vectores.		X	X	
2.45	La solución debe incluir modelos de detección predefinidos que combinen múltiples reglas y filtros que utilicen técnicas como el aprendizaje automático y el apilamiento de datos. Debe actualizarse periódicamente para mejorar la detección de amenazas y reducir las alertas de falsos positivos.		X	X	
2.46	La solución debe tener la capacidad de habilitar o deshabilitar modelos de detección y agregar y configurar excepciones de modelos de detección según los requisitos de la organización.		X	X	
2.47	La solución debe permitir la creación de modelos de detección personalizados y filtros de eventos personalizados que definan los eventos que el modelo utiliza para activar alertas.		X	X	
2.48	La solución debe poder analizar y determinar si ciertos indicadores señalan un ataque en curso, lo que permitirá al equipo SOC tomar medidas oportunas de prevención, investigación y mitigación contra campañas de ataques específicos.		X	X	
2.49	La solución debe enumerar todos los eventos asignados al marco MITRE ATT&CK; con el fin de que el analista SOC puede usar estos eventos como punto de partida para realizar investigaciones adicionales.		X	X	
2.50	La solución debería proporcionar más contexto con mapeo a los TTP (Técnicas, Tácticas y Procedimientos) MITRE ATT&CK para una detección más rápida y alertas de mayor fidelidad.		X	X	
2.51	La solución debe tener la capacidad de escribir consultas de búsqueda personalizadas, agregar las consultas guardadas a la lista de seguimiento y ejecutarlas automáticamente contra los últimos datos de telemetría en un intervalo.		X	X	
3.	**ADMINISTRACIÓN**				
3.1	La solución debe ser compatible con el acceso basado en roles (RBAC) para la administración de derechos de acceso a la consola		X	X	
3.2	La solución puede distinguir el acceso a funciones y parámetros según los roles.		X	X	
4.	**ALERTAS**				
4.1	La solución debe poder notificar a un administrador en función de un umbral personalizado con el fin de evitar fatigas de alertas		X	X	
4.2	La solución debe poder notificar a un destinatario interno en caso de correo electrónico en cuarentena / eliminado / limpiado		X	X	
4.3	La solución debe poder enviar eventos de alerta por correo electrónico al SIEM QRadar		X	X	
5.	**REPORTES**				
5.1	La solución debe conservar los registros (usuario y		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	administrador) durante al menos 3 meses				
5.2	La solución debe poder mostrar el panel del día, la semana o el mes actual con: 1.El número de correos electrónicos analizados, no analizados, sospechosos, bloqueados, en cuarentena. 2. El tiempo promedio de escaneo, particularmente en el tiempo de análisis de sandboxing. 3. El nivel de riesgo de los correos electrónicos sospechosos. 4. El top 10 de malware detectado. 5. El top 10 de buzones con actividad sospechosa.		X	X	
6.	CAPACIDADES DE DETECCIÓN Y RESPUESTA EN OFFICE 365 PARA LA ATENCIÓN DE INCIDENTES				
6.1	Extended Detection and Response (XDR) debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.		X	X	
6.2	Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis entre ellas Data Stacking y Machine Learning.		X	X	
6.3	La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.		X	X	
6.4	La solución deberá contar con una interfaz visual de correlación e investigación que centralice, agrupe y correlacione automáticamente los eventos de seguridad, utilizando capacidades de inteligencia artificial, enriquecida con inteligencia de amenazas y alineada con las tácticas y técnicas del marco MITRE ATT&CK, permitiendo visualizar de forma gráfica el linaje de los eventos, las comunicaciones de red y el impacto sobre los activos comprometidos.		X	X	
6.5	Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.		X	X	
6.6	Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).		X	X	
6.7	Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.		X	X	
6.8	XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.		X	X	
6.9	Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz para ver las accionas que una amenaza llevó a cabo en un correo de Office 365		X	X	
6.10	Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el fabricante		X	X	
6.11	La capacidad de Inteligencia de Amenazas (Threat Intelligence) embebida debe ser capaz de identificar la campaña asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.		X	X	
6.12	La solución debe tener un chatbot impulsado por IA para guiar las investigaciones y brindar respuestas automáticas a cualquier pregunta relacionada con la ciberseguridad.		X	X	
6.13	La solución debe tener la capacidad de agregar o eliminar		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	indicadores de compromiso admitidos a la lista de bloqueo, incluidos, entre otros, hash de archivo, URL, dirección IP y dominios.				
6.14	La solución debe ofrecer un enfoque holístico a la seguridad del correo electrónico con protección diseñada específicamente para aplicaciones de correo electrónico y colaboración, y enriquecida con XDR y capacidades de gestión de exposición al riesgo cibernético.		X		X
6.15	La solución debería tener la capacidad de mover el mensaje de correo electrónico seleccionado a la carpeta de cuarentena y poner en cuarentena el mensaje de todos los buzones afectados.		X	X	
6.16	La solución debería tener la capacidad de eliminar el mensaje de correo electrónico seleccionado de los buzones seleccionados.		X	X	
6.17	La consola debe proporcionar diferentes métodos de búsqueda, filtros y un lenguaje de consulta fácil de usar para identificar, categorizar y recuperar resultados de búsqueda.		X	X	
7.	**GESTIÓN DE MODELOS DE DETECCIÓN**				
7.1	Los modelos de detección deben consistir en uno o más conjuntos de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK		X	X	
7.2	El fabricante debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos.		X	X	
7.3	Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).		X	X	
7.4	La solución deberá permitir a los administradores habilitar, deshabilitar y ajustar la sensibilidad de los modelos de detección, así como configurar de manera granular los criterios de envío de alertas hacia la consola de investigación y correlación, basándose en niveles de severidad, categorías de amenaza y grado de confianza del modelo, con el objetivo de optimizar los tiempos de detección y respuesta del equipo de seguridad.		X		X
7.5	Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE. Critico: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. Alto: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medio: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Bajo: Hay indicadores levemente sospechosos. Usado para monitoreo y caza de amenazas (Threat Hunting).		X		X
7.6	Los modelos deben especificar y permitir modificar el estado: encendido/apagado		X	X	
7.7	Los modelos deben especificar la última vez que se actualizó		X	X	
8.	**AUTOMATIZACIÓN**				
8.1	La solución debe contar con la capacidad de enviar alertas por medio de la integración de webhooks. Las alertas deberán ser configurables por nivel de severidad,		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	permitiendo que solo las alertas clasificadas como 'altas' o 'críticas' sean enviadas, mientras que las alertas informativas se mantengan exclusivamente en la consola central.				
8.2	La solución debe contar con la capacidad de generar una serie de flujo de procesos que permita tomar acciones de respuesta automatizadas por medio de las fuentes propias o Tecnologías de tercero que permitan dependiendo de la capa de seguridad tomar una acción de respuesta, para el caso de correo e identidad, mandar a cuarentena el mensaje, o forzar a cerrar sesión a la identidad, forzar a reiniciar la contraseña, entre otros.		X	X	
9. ADMINISTRACIÓN					
9.1	La configuración administrativa de XDR debe brindar a los usuarios la capacidad de configurar cuentas de usuario, roles y configuraciones, conectar productos adicionales y configurar opciones de monitoreo adicionales. Las siguientes opciones deben estar disponibles:		X	X	
9.2	**1.** SAML Single Sign-On: Debe soportar inicio de sesión SAML, single sign-on (SSO) utilizando las credenciales corporativas. **2.** Gestión de Cuenta: Debe permitir crear usuarios locales y usuarios para aplicaciones de terceros que se conectan a la API. **3.** Gestión de Role: Debe permitir ver y configurar el acceso basado en roles que se aplican a los usuarios aplicativos de terceros que se conectan a través de la API **4.** Conector de Producto: Debe permitir conectar de manera nativa el correo, y de manera alternativa los puntos finales, servidores, Nube, y productos de red. **5.** Logs de Auditoria: Debe proveer logs de auditoría que provee un resumen de acceso de usuario, acciones relacionadas con las Apps, cambio de configuraciones, y otras modificaciones que ocurran usando la consola XDR o las APIs. **6.** Soporte Remoto: debe permitir a los ingenieros de Soporte acceder a la consola de XDR para resolución de problemas y recolección de "debug logs" si es necesario.		X	X	
10. GESTÓN Y OPERACIÓN					
10.1	La solución debe poder consolidar la protección de correo electrónico SaaS, local, de puerta de enlace y API en una única plataforma integrada.		X	X	
10.2	La solución debe proporcionar una plataforma centralizada de visibilidad y gestión en soluciones de correo electrónico basadas en API y gateway.		X		X
10.3	La solución debe proporcionar un inventario de activos de correo electrónico y poder mostrar los activos de correo electrónico de la organización, incluidas todas las cuentas de correo electrónico y todas las cuentas de dominio		X	X	
10.4	Debe poder identificar a los usuarios más específicos de la organización y configurar políticas de acceso condicional para los usuarios riesgosos.		X	X	
10.5	La solución debe tener la capacidad de automatizar una variedad de acciones utilizando manuales de seguridad para ayudar a reducir la carga de trabajo y acelerar las tareas de seguridad y las investigaciones.		X		X
10.6	La solución debe poder descifrar y escanear mensajes de		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	correo electrónico y archivos adjuntos cifrados con MIP en Exchange Online y archivos cifrados con MIP en SharePoint, OneDrive y MS Teams.				
10.7	La solución debe tener un panel altamente personalizable que proporcione widgets que muestren estadísticas de superficie de ataque, correo electrónico, identidad, entre otros.		X	X	
10.8	La solución debe ofrecer una integración de detección y respuesta de correo electrónico (Email DR) y Gestión de exposición de Riesgos		X	X	
10.9	La solución debe poder mostrar el mapeo MITRE ATT&CK de las tácticas y técnicas detectadas en la organización para las siguientes matrices MITRE ATT&CK. Empresa (Enterprise) Móvil (Mobile) ICS		X	X	
11. REQUERIMIENTOS DE LA PLATAFORMA					
11.1	La solución debe proporcionar una plataforma unificada que permita a los equipos de seguridad ejecutar un análisis de causa raíz, investigar el perfil de ejecución de un ataque e identificar el alcance del impacto en los activos.		X	X	
11.2	La solución debe incluir un período estándar de retención de Alertas de Investigación y Correlación y registros de detección y actividad presentada en la funcionalidad de Correo y aplicaciones de colaboración, no menor a 180 días.		X	X	
11.3	La solución debería ofrecer una opción para ampliar la retención de datos hasta 365 días.		X	X	
11.4	El fabricante deberá estar certificado con las siguientes normas internacionales de cumplimiento las cuales a su vez deberán dar alcance a la solución de seguridad a licenciar: ISO 27001 (Para lo cual se deberá anexar soporte directo firmado por ente certificador) ISO 27014 (Para lo cual se deberá anexar soporte directo firmado por ente certificador) ISO 27017 (Para lo cual se deberá anexar soporte directo firmado por ente certificador) SOC 2 o SOC 3 (la Entidad aceptará la entrega de "Bridge Letters" (Cartas de Continuidad) o documentos equivalentes emitidos por el fabricante o su firma auditora, siempre que estos certifiquen que el entorno de control de la solución no ha sufrido cambios significativos desde el último periodo de auditoría, garantizando así la idoneidad técnica durante todo el proceso de contratación)		X No anexo soportes solicitados	X CERTIFICACION ISO -27001-27014-27034 certificate.pdf en-globalCERTIFICACION ISO - 27017-certificate.pdf SOC2_Bridge_Letter_Apr_2026.pdf	
12. INTEGRACIÓN CON TERCEROS Y API					
12.1	La solución debe poder integrarse con la funcionalidad de Protección de Información de Microsoft (MIP) para descifrar y escanear correos electrónicos y archivos cifrados con MIP.		X	X	
12.2	La solución debe poder integrarse con productos SIEM y SOAR comunes.		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
12.3	La solución debe poder integrarse con soluciones IdP de terceros para los requisitos de inicio de sesión único (SSO).		X	X	
12.4	La solución debería poder generar claves API mediante control de acceso basado en roles para permisos más granulares. Las claves API deberían poder caducar y desactivarse desde la consola de administración.		X	X	
12.5	La solución también debe tener la capacidad de integrarse con otras soluciones de terceros a través de API.		X	X	
12.6	La solución debe proporcionar conectores listos para integrarse con otras soluciones de seguridad de terceros compatibles		X	X	
12.7	La solución debe ser integrable con al menos una solución de terceros de la siguiente categoría: Firewall Fortinet Firewall Paloalto SIEM QRadar Directorio Activo		X	X	
13. GESTIÓN DEL RIESGO					
13.1	El contratista debe ofrecer una solución que realice un análisis continuo y en tiempo real de todos los activos de la organización especialmente del correo electrónico, permitiendo una visión integral del riesgo de ciberseguridad. Se requiere: 1. Correlación unificada de telemetría desde múltiples fuentes. 2. Evaluación integral de riesgos. 3. Visibilidad de la superficie de ataque, incluyendo activos expuestos a Internet. 4. Puntuación de riesgo contextualizada, considerando la criticidad y la exposición de los activos.		X	X	
13.2	La solución debe contar con capacidades de inteligencia de amenazas en tiempo real para prevenir, detectar y priorizar vulnerabilidades críticas antes de que sean explotadas. Se requiere: 1. Integración con una iniciativa global de Zero Day (ZDI) para la detección temprana de vulnerabilidades. 2. Priorización basada en explotación activa en el mundo real, no solo en criticidad teórica. 3. Correlación automática con intentos de explotación detectados 4. Análisis de configuraciones incorrectas en múltiples plataformas.		X	X	
13.3	El contratista debe ofrecer una solución que permita actuar sobre los riesgos detectados sin intervención manual, asegurando una reducción proactiva de la superficie de ataque. Se requiere: 1. Recomendaciones accionables para mitigación inmediata de riesgos. 2. Playbooks de respuesta automatizados para la remediación de vulnerabilidades. 3. Integración con soluciones de control de acceso para respuesta automática ante amenazas. 4. Capacidad de personalización de reglas de riesgo. 5. Métricas de mejora de postura de seguridad en el tiempo.		X	X	
13.4	La plataforma debe proporcionar una vista centralizada del		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	riesgo organizacional con métricas claras y accionables para la toma de decisiones estratégicas. Se requiere: 1. Vista unificada de los riesgos de la organización, sin necesidad de múltiples herramientas. 2. Métricas comparativas con la industria, permitiendo evaluar el nivel de seguridad frente a otros sectores. 3. Seguimiento de tendencias de riesgo en tiempo real. 4. KPIs de reducción de riesgo, con mediciones tangibles de mejora de seguridad. 5. Visualización dinámica de la superficie de ataque, permitiendo identificar activos críticos expuestos.				
13.5	El contratista debe garantizar que se cuente con capacidades avanzadas de análisis de riesgos en múltiples capas de seguridad. Se requiere: 1. Evaluación de riesgos en buzones de correo en la nube, detectando configuraciones inseguras o accesos sospechosos. 2. Detección de anomalías en comportamiento de usuarios, identificando accesos o actividades fuera del patrón normal.		X	X	
13.6	La solución debe poder gestionar todos los activos descubiertos desde una única consola de gestión unificada.		X	X	
13.7	La solución debe poder integrarse con proveedores externos para incorporar o enriquecer datos de la superficie de ataque.		X	X	
13.8	La solución debe contar con la capacidad de tener embebido un apartado para identificar la postura de identidad a través de la integración con el AD, generando un índice numérico de riesgo que permita identificar cuáles usuarios tiene MFA deshabilitado, contraseña no robusta, política de expiración de contraseña deshabilitado, y eventos de riesgo (Viajes imposibles, volcado de credenciales, credenciales filtradas a la dark web, ataque de fuerza bruta, etc).		X	X	
13.9	La solución debe contar con la capacidad de tener una funcionalidad para realizar barridos de indicadores de compromiso (IOC's) basado en más de 30.000 reportes de la marca y fuentes de terceros (Entidades gubernamentales, centros de investigación, etc.) para confirmar si hay alguna amenaza en el ambiente que se empareje con estos reportes, y poder identificar el activo afectado.		X	X	
13.10	La solución debe ser capaz de identificar si la organización está por encima, por debajo o en promedio del nivel de riesgo de compañía a nivel de sector industrial, tamaño organizacional o regional.		X	X	
13.11	La solución debe ser capaz de modificar la criticidad de un activo en función de la necesidad de la compañía.		X	X	
13.12	La solución debe tener soporte integrado para manuales de seguridad que puedan usarse para la remediación automatizada.		X	X	
13.13	La solución debe poder evaluar la situación de seguridad de Internet y otros activos externos de la organización (Gestión de la superficie de ataque externa).		X	X	
13.14	La solución debe proporcionar una puntuación de riesgo para toda la organización basada en una evaluación		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	continua de los riesgos en la organización.				
13.15	Incorpore la criticidad de los activos, las vulnerabilidades, la actividad de amenazas y la configuración de los controles de seguridad en el cálculo del puntaje de riesgo para cada tipo de activo.		X	X	
13.16	La solución debe proporcionar un índice de exposición que resuma la probabilidad de que se produzca una vulnerabilidad o amenaza en el entorno.		X	X	
13.17	Debe utilizar múltiples proveedores de datos de descubrimiento (la dependencia del agente existente debe complementarse con proveedores de descubrimiento adicionales).		X	X	
13.18	La solución debe proporcionar métricas de gestión de vulnerabilidades para activos internos y de acceso a Internet a lo largo del tiempo y permite comparar la puntuación de las organizaciones con el promedio global. Métrica: CVE únicos altamente explotables.		X	X	
13.19	La solución debe proporcionar métricas de gestión de vulnerabilidades para activos internos y de Internet a lo largo del tiempo y permite comparar la puntuación de las organizaciones con el promedio global. Métrica: Tiempo promedio sin parches.		X		X
13.20	La solución debe proporcionar la función de poder identificar aquellos riesgos de mayor prioridad para mitigar basado en la meta que el cliente desee abordar para disminuir el número de riesgo, y así, la solución deba calcular basado en la métrica ingresada por el cliente, lograr mostrarte los riesgos de mayor foco a mitigar.		X		X
13.21	Debe proporcionar información sobre la postura de seguridad de la organización mediante un panel de control de nivel ejecutivo. Debe poder mostrar la puntuación de riesgo general de la empresa, los riesgos de los activos individuales, una vista de los ataques en curso y sus factores de riesgo contribuyentes.		X		X
13.22	Los informes se pueden generar por demanda o mediante programación.		X	X	
13.23	El contenido de los informes se puede filtrar para limitar la salida según criterios seleccionados		X	X	
13.24	Debe proporcionar la capacidad de la vista de inventario y de operaciones tener la facilidad de realizar filtros por diferentes tipos de información (Tipo de Activo, qué tecnología lo descubrió, índice de riesgo, etc).		X	X	
13.25	La solución debe ser considerada líder en el segmento de gestión de exposición de ciber-riesgos por alguna firma global reconocida en investigación y consultoría en tecnología de la información.		X	X	
14. SOPORTE DEL FABRICANTE					
14.1	El fabricante como mínimo debe: • Brindar soporte telefónico y basado en la web • Permitir la generación de casos a través del teléfono y del portal de soporte las 24 horas del día, los 7 días de la semana • brinda soporte técnico las 24 horas para problemas urgentes (críticos), mientras que las consultas y problemas no críticos deben ser atendidos durante el horario comercial habitual • Soportar la instalación y actualización de	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	productos • brindar transferencia de conocimiento para mínimo 4 personas por 20 horas y acceso a base de conocimientos (*knowledge base*) y mejores prácticas • Análisis de archivos sospechosos • Actualizaciones y mejoras de la solución	SA 020-2026 – I.pdf		Copy.pdf	
15.	**TIEMPOS DE RESPUESTA Y SEVERIDAD**				
15.1	El fabricante como mínimo debe cumplir con: Severidad 1 (Crítica): Dentro de 1 hora. Se aplica cuando los componentes principales del producto quedan inoperables, hay un impacto crítico en las operaciones del negocio y no existe una solución alternativa (workaround). ◦ Nota: Debe enviarse por teléfono (o en línea seguido inmediatamente de una llamada). • Severidad 2 (Alta): Dentro de 4 horas hábiles locales. Se aplica cuando los componentes principales están severamente deteriorados o degradados, causando un impacto significativo en las operaciones comerciales. • Severidad 3 (Media): Dentro de 1 día hábil local. Se aplica cuando la funcionalidad del producto está afectada pero operativa, o hay fallos en componentes no esenciales. El impacto en el negocio es medio o bajo y existe una solución alternativa. • Severidad 4 (Baja): Dentro de 2 días hábiles locales. Se utiliza para problemas leves, solicitudes de mejoras, preguntas generales o incidentes con poco o nulo impacto en la DIPOL	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
16.	**NIVEL DE EDUCACION O NIVEL ACADEMICO**				
16.1	Un profesional Ingeniero Electrónico, de Sistemas o Telecomunicaciones, con mínimo 2 años de experiencia contada a partir de la expedición de la tarjeta profesional, este se deberá acreditar anexando a la propuesta acta de grado y diploma con su tarjeta profesional vigente. Dentro de los dos años de experiencia se debe acreditar experiencia de seis (6) meses, en configuración y mantenimiento en soluciones de seguridad informática la cual se acreditará anexando certificación firmada por el oferente o el fabricante, y Especialización en Seguridad de la Información o Informática la cual se acreditará anexando acta de grado y diploma. Certificaciones Mínimas: - Profesional certificado por el fabricante de la solución ofertada, con certificación vigente de nivel avanzado (Advanced) en la herramienta solicitada. (anexar certificación) - CEH (Certified Ethical Hacker) vigente (anexar certificación) - CISP- Certified Information Security Professional (anexar certificación) **Nota:** para personal que haya obtenido su título por fuera del país, tendrá que demostrar la convalidación de este ante el Ministerio de Educación, teniendo en cuenta la Ley		X No se evidencia que se relacione en la propuesta el personal solicitado		X

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	842 de 2003 Articulo 6 y la Circular Externa Única de Colombia Compra Eficiente, Ítem 9.3 Acreditación de la formación académica.				
16.2	Un profesional Ingeniero electrónico, de sistemas o Telecomunicaciones, este se deberá acreditar anexando a la propuesta acta de grado y diploma con su tarjeta profesional vigente. Este profesional deberá contar con Magister en Ciberseguridad y Ciberdefensa que deberá ser acreditado anexando acta de grado y diploma. Este profesional deberá contar con mínimo 3 años de experiencia contada a partir de la expedición de la tarjeta profesional. Adicionalmente el oferente o fabricante deberá certificar experiencia de este profesional gerenciando proyectos de Ciberseguridad. Certificaciones mínimas - Project Management Professional – PMP (anexar certificado) - Scrum Master Professional Cerfificate (anexar certificado) - **Nota:** para personal que haya obtenido su título por fuera del país, tendrá que demostrar la convalidación de este ante el Ministerio de Educación, teniendo en cuenta la Ley 842 de 2003 Articulo 6 y la Circular Externa Única de Colombia Compra Eficiente, Ítem 9.3 Acreditación de la formación académica.		X No se evidencia que se relacione en la propuesta el personal solicitado	X JORGE HERNANDO PORRAS GONZALEZ ActaGrado-IngenieroSistemas.pdf DocumentosAcademicos.pdf Tarjeta o matricula profesional Jorge Porras.pdf ActaGrado MaestriCSCD.pdf Certificación Laboral Jorge Porras.pdf CertificacionPMP.pdf CertificacionesScrum.pdf	
16.3	Un Técnico o tecnólogo en sistemas, telecomunicaciones, electrónica o afines, este se acreditará anexando acta de grado y diploma. Deberá contar con mínimo dos años de experiencia en configuración y mantenimiento en soluciones de seguridad informática. Certificaciones Mínimas: - Profesional certificado por el fabricante de la solución ofertada, con certificación vigente de nivel avanzado (Advanced) en la herramienta solicitada. (anexar certificación) - **Nota:** para personal que haya obtenido su título por fuera del país, tendrá que demostrar la convalidación de este ante el Ministerio de Educación, teniendo en cuenta la Ley 842 de 2003 Articulo 6 y la Circular		X No se evidencia que se relacione en la propuesta el personal solicitado	X JORGE LUIS CEPEDA SANABRIA Diploma Tecnico.pdf Acta de grado Tecnico.pdf Certificacion Advanced email - Jorge Cepeda.jpe	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	Externa Única de Colombia Compra Eficiente, Ítem 9.3 Acreditación de la formación académica.			g	
17.	**CERTIFICACIONES ADICIONALES**				
17.1	Certificación de Partner en alguno de los dos niveles más altos, expedida por el fabricante de la solución propuesta no mayor a treinta (60) días anteriores al cierre del proceso, en la que conste que el proponente cuenta con la calidad de canal oficial y que certifique venta y distribución de la solución propuesta		X No se anexo certificación solicitada	X TM_17.2026_-_DIPOL_-_Carta_Partner_HIGH_TECH_SERVICES_.docx.pdf	
18.	**EXPERIENCIA**				
18.1	Con el fin de garantizar la calidad de los servicios a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en la clasificación 43222600 y/o 43222500 y/o 43233200 y/o 81112200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a superior a 158,66 S.M.M.L.V, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		X No anexo registro único de proponentes		X No tiene el RUP actualizado a la vigencia.
19.	**GARANTÍA TECNICA**				
19.1	El contratista frente a la celebración de contratos de software o licenciamiento, tendrá que entregar ***certificados de autenticidad, el certificado de distribuidor autorizado y las facturas*** los cuales deberán ser entregados durante la ejecución del contrato, previo acuerdo con el supervisor del mismo.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
19.2	El contrato tendrá su ejecución hasta el 10 agosto del 2026 y deberá contar con una garantía de treinta y tres (33) meses después de la finalización de su ejecución.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
19.3	El contratista deberá proporcionar soporte técnico durante los treinta y tres (33) meses siguientes a la finalización de la ejecución del contrato, atendiendo cualquier requerimiento formulado por los funcionarios de la DIPOL, así como los incidentes que afecten el normal	X ANEXO No. 2-8 ESPECIFICACIONE		X ANEXO No. 2-8 ESPECIFICACIONES	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	funcionamiento de la plataforma poniendo a disposición el personal calificado y los recursos necesarios para su resolución conforme al alcance contractual; los casos reportados deberán ser atendidos en un tiempo de seis (6) horas y resueltos en un plazo máximo de veinticuatro (24) horas contadas a partir de su notificación. En los casos de requerirse aumentar este tiempo, se debe elaborar por parte de la empresa contratada un informe estableciendo el cronograma de respuesta y los motivos.	S Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
19.4	En caso de presentarse indisponibilidad total del servicio durante el periodo de garantía, la empresa contratista deberá atender el soporte en sitio, en un tiempo de respuesta de máximo cuatro (4) horas, hasta restablecer el servicio.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
19.5	Durante el período de garantía, el contratista deberá realizar un mínimo de once (11) visitas de seguimiento, revisión, actualización u mejoras sobre el software que compone la solución de seguridad. Estas visitas deberán ser programadas según la necesidad y de común acuerdo con el administrador de la herramienta tecnológica en DIPOL, garantizando al menos una (1) visita trimestral.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20. SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO					
20.1	El oferente deberá entregar en la oferta el documento firmado por el representante legal el cual indique el número de trabajadores permanentes, el nivel de riesgo de su principal actividad económica y asimismo anexar la calificación de los estándares mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo de la vigencia anterior, lo anterior como consideración a la Resolución 0312 del 13 de febrero del 2019 del Ministerio de Trabajo "*Por la cual se definen los Estándares Mínimos del Sistema de Gestión de SST*", en cumplimiento al art. 1 la presente Resolución tiene por objeto establecer los Estándares Mínimos del SG-SST para las personas naturales y jurídicas señaladas en el art. 2 aplica a los empleadores públicos y privados, a los contratantes del personal bajo modalidad de contrato civil, comercial o administrativo, a los trabajadores dependientes e independientes, a las organizaciones de economía solidaria y del sector cooperativo a las agremiaciones u asociaciones que afilian trabajadores independientes al sistema de seguridad social integral, a las empresas de servicios temporales, a los estudiantes afiliados al Sistema		X No anexo el documento solicitado.	X SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO. pdf	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	General de Riesgos Laborales y los trabajadores en misión; a las administradoras de riesgos laborales; a la Policía Nacional en lo que corresponde a su personal no uniformado y al personal civil de las Fuerzas Militares; quienes deben implementar los Estándares Mínimos del Sistema de Gestión de SST en el marco del Sistema de Garantía de Calidad del Sistema General de Riesgos Laborales.				
20.2	El contratista deberá entregar al supervisor del contrato los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.3	En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al supervisor del contrato, con el fin de que este haga llegar la copia al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución **1401** del **14/05/2007** del Ministerio de Trabajo y Protección Social "*Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo*" o cualquiera que la modifique, reemplace o sustituya.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.4	El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.5	En caso de presentarse una emergencia dentro de las instalaciones durante el desarrollo del objeto contractual, el contratista deberá garantizar que el personal bajo su mando, atienda las recomendaciones durante la activación del plan de emergencia de las instalaciones policiales.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
		2026 – I.pdf			
20.6	En caso de que se desarrolle en la Dirección de Inteligencia Policial una auditoría del SG-SST durante la ejecución del contrato, el contratista deberá suministrar al supervisor del contrato la documentación requerida del objeto contractual.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.7	El contratista garantizará que el personal que ingrese a las instalaciones se encuentre con la debida identificación de la empresa.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
21. REQUERIMIENTOS AMBIENTALES					
21.1	El contratista deberá cumplir con la normatividad ambiental vigente nacional para reducir los aspectos e impactos ambientales asociados a la actividad y aplicación de buenas prácticas ambientales.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
21.2	Desarrollar y cumplir, durante la vigencia y ejecución del objeto del contrato, con las buenas prácticas ambientales con relación al ahorro y uso eficiente del agua y la energía, así como el manejo integral de residuos (no peligrosos y peligrosos), establecidas por la Dirección y el marco del mantenimiento del Sistema de Gestión Ambiental en las instalaciones del contratante; que contribuyan al cumplimiento de la política ambiental y objetivos ambientales institucionales.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22. CUMPLIMIENTO CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN					

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
22.1	El contratista acatará los controles establecidos para la seguridad de la información en la Dirección de Inteligencia Policial, así como la firma del compromiso de reserva y la aplicación de los estudios de credibilidad y confiabilidad. Para ello el personal que realice la instalación o configuración, así como las actividades de soporte técnico de equipos y sistemas, deberá cumplir con un estudio de confiabilidad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato y el tiempo de la garantía técnica. En el evento de no aprobar dicho estudio algunas de las personas vinculadas a este proyecto, el contratista deberá realizar el cambio de estas personas por otras que también deberán cumplir con el estudio de confiabilidad requerido.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.2	Cláusula de Confidencialidad: Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el transcurso del proyecto, será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata, se considera también información confidencial: a) aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes. b) la que no sea de fácil acceso, y c) aquella información que no esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial, duración. El acuerdo regirá durante el tiempo que dure el proyecto, derechos de propiedad, toda información intercambiada es de propiedad exclusiva de la parte de donde proceda. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso, modificación o terminación. El acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.3	Confidencialidad e integridad de la información institucional: Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la preservación de la integridad y confidencialidad de la información institucional a la cual llegare a tener acceso directamente o por intermedio de terceros; en tal virtud, adoptará todas las medidas que sean necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida y suscribirá con la entidad los formatos de confidencialidad o reserva a que haya lugar por el termino establecido en la ley estatutaria 1621 de 2013.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.4	En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del futuro contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de la labor. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información para lo cual deberá diligenciar el formulario establecido por la entidad contratante. El manejo de toda la información de	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	arquitectura del sistema se considera CONFIDENCIAL, de manera que los planos, diseño, manuales técnicos y cualquier otro tipo de información estarán limitados únicamente a la interventora o supervisión. El suministro de copias para otras personas o entidades deberá ser solicitada a la DIRECCIÓN DE INTELIGENCIA DE LA POLICÍA NACIONAL.	PN DIPOL SA 020-2026 – I.pdf		SA 020-2026 - I Copy.pdf	
22.5	El contratista y todo el personal que realice la instalación y configuración de los equipos, cumplirá los protocolos descritos en el Manual del Sistema de Gestión de Seguridad de la Información de la Policía Nacional y el instructivo vigente mediante el cual se establece el Protocolo de Seguridad de la Información para el Servicio de Inteligencia Policial, debiendo suscribir el compromiso de reserva y el de confidencialidad.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.6	Durante el desarrollo de la instalación y configuración, el contratista se compromete a no hacer uso indebido de las herramientas de software o hardware utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	

RESUMEN DE LA EVALUACIÓN TÉCNICA

Resumen de la evaluación REALTIME CONSULTING & SERVICES S.A.S:

La empresa REALTIME CONSULTING & SERVICES S.A.S, **NO CUMPLE** con todos los requisitos técnicos exigidos dentro del proceso PN DIPOL SA 020-2026, cuyo objeto es la "ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL", específicamente en los siguientes ítems del pliego de condiciones técnicas mínimas y ficha técnica:

Ítem 1.2 al ítem 11.3 y del ítem 12.1 al ítem 13.25: No se puede evaluar el cumplimiento de los anteriores ítems, toda vez, que no se especificó la marca, referencia y fabricante de la solución ofertada, sin poder establecer lo requerido en el anexo de especificaciones y ficha técnica.

Ítem 11.4: El oferente no anexó a su propuesta las certificaciones y documentos exigidos de las normas internacionales solicitadas.

Ítem 16.1 al ítem 16.3: El oferente no los documentos del personal que cumpla con los títulos y certificaciones exigidas.

Ítem 17.1.: El oferente no adjuntó la certificación de partner en los niveles requeridos, expedida por el fabricante de la solución ofertada.

Ítem 18.1.: El oferente no adjuntó el Registro Único de Proponentes (RUP).

Ítem 20.1.: El oferente no anexó los documentos exigidos en el presente proceso indicando el número de trabajadores permanentes, el nivel de riesgo de su principal actividad económica y asimismo no anexó la calificación de los estándares mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo de la vigencia anterior.

Resumen de la evaluación HIGH TECH SERVICES CORP (HTS CORP) S.A.S.:

La empresa HIGH TECH SERVICES CORP (HTS CORP) S.A.S., **NO CUMPLE** con todos los requisitos técnicos exigidos dentro del proceso PN DIPOL SA 020-2026, cuyo objeto es la "ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL", específicamente en los siguientes ítems del pliego de condiciones técnicas mínimas y ficha técnica:

Ítems 2.6 al 2.16, 2.19, 2.28, 2.29, 2.31, 2.32, 2.35, 2.42, 6.14, 7.4, 7.5, 10.2, 10.5, 13.19 al 13.21: El Comité Técnico no logra establecer el cumplimiento de los ítems anteriormente descritos, dado que no se adjuntó ni fue posible identificar, dentro de la información pública en las páginas oficiales del fabricante ofertado, documentación técnica que los respalde, tales como hojas de datos (datasheets), fichas técnicas, descripciones funcionales u otra información oficial relacionada con las capacidades requeridas.

En consecuencia, se solicita al oferente suministrar documentación técnica oficial que permita la verificación objetiva de dichas funcionalidades. Asimismo, deberá indicarse de manera expresa **la fuente y la ubicación exacta dentro de la documentación aportada** (por ejemplo: nombre del documento, sección, capítulo, página, tabla o referencia específica) en la que se evidencie el cumplimiento de cada requisito.

Adicionalmente, en aquellos casos en los que la denominación de la funcionalidad o módulo no corresponda de forma directa con el atributo solicitado, el oferente deberá justificar técnica y detalladamente con qué característica de la solución se satisface la especificación requerida.

Ítem 16.1: No se adjuntó acta de grado del título profesional para el señor EDWIN DANILO VELASCO CALDAS, toda vez, que el documento aportado con el nombre "ACTA DE GRADO INGENIERIA DE TELECOMUNICACIONES.jpeg", no se puede tener en cuenta al ser una certificación.

De la misma manera no anexó certificaciones de experiencia expedidas por el **oferente o fabricante**, es de anotar que no se tienen en cuenta los documentos anexados "Certificación Experiencia Edwin.pdf" y "Certificacion TI360 Edwin Velasco.pdf", por cuanto las expiden empresa externas, sin considerar lo solicitado en el ítem.

Ítem 18.1: No se puede evaluar la experiencia por cuanto no se aportó Registro Único de Proponentes actualizado.

En razón de lo anterior, las empresas podrán subsanar en los términos y tiempos establecidos para el presente proceso, la documentación citada en las especificaciones técnicas.

COMITÉ ECONÓMICO: mediante comunicación oficial GS-2026-016147-DIPOL del 22/04/2026, presentó la siguiente respuesta:

DOCUMENTOS DE VERIFICACIÓN DE CARÁCTER ECONÓMICO

PROPONENTE	DOCUMENTOS		
	CERTIFICACIÓN BANCARIA	FORMULARIO No. 2	OBSERVACIONES
REALTIME CONSULTING Y SERVICES SAS	CUMPLE	CUMPLE	-
HIGH TECH SERVICES CORP (HTS CORP) S.A.S	CUMPLE	CUMPLE	-

INDICADORES FINANCIEROS

PROPONENTE	REFERENCIA DE INDICADORES				
	ÍNDICE DE LIQUIDEZ *(Menor a 1,57 es excluyente)*	ÍNDICE ENDEUDAMIENTO *(Mayor a 0,71 excluyente)*	*ÍNDICE RAZÓN DE COBERTURA DE INTERÉS (Menor a 1 excluyente)*	ÍNDICE RENTABILIDAD DEL ACTIVO *(Menor a 0,05 excluyente)*	ÍNDICE RENTABILIDAD PATRIMONIO *(Menor a 0,09 excluyente)*
REALTIME CONSULTING Y SERVICES SAS	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE
HIGH TECH SERVICES CORP (HTS CORP) S.A.S	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE

RESUMEN DE LA EVALUACIÓN ECONÓMICA

PROPONENTES	OBSERVACIONES
REALTIME CONSULTING Y SERVICES SAS	En atención a que el proponente NO anexó el RUP, el cual se encuentra establecido dentro de los pliegos definitivos en el ítem 1.3 **Requisitos Económicos Habilitantes desde el numeral 1.3.2 hasta el 1.3.5** *"El oferente deberá anexar el registro único de proponentes - RUP, tener en cuenta que de acuerdo con lo señalado en el artículo 2.2.1.1.1.5.1. del Decreto 1082 de 2015, la renovación de este registro debe realizarse entre el 1° de enero y a más tardar el quinto (5) día hábil del mes de abril de cada año. De lo contrario, cesarán los efectos, no podrán solicitar certificado y deberán realizar una nueva inscripción".* Por lo anterior, se requiere que el oferente remita el RUP, con el fin de verificar el cumplimiento de los indicadores financieros dentro de los plazos establecidos.
HIGH TECH SERVICES CORP (HTS CORP) S.A.S	Para determinar el cumplimiento de los indicadores financieros se revisó el Registro Único de Proponentes – RUP allegado por parte del oferente, evidenciándose que el mismo presenta como fecha de renovación el 09/04/2025; motivo por el cual no se puede hacer la valoración de los indicadores en mención de la vigencia 2025. Frente a lo anterior, se observa que la capacidad financiera y organizacional del proponente, presentan un reporte a corte 31/12/2024.  CERTIFICA: IDENTIFICACION QUE: HIGH TECH SERVICES CORP (HTS CORP) S.A.S. NIT: 901121717 1 NUMERO DEL PROPONENTE EN LA CAMARA DE COMERCIO: 00969351 CERTIFICA: INSCRIPCION Y RENOVACION FECHA DE INSCRIPCION EN EL REGISTRO DE LOS PROPONENTES: 2020/07/29 FECHA DE ULTIMA RENOVACION EN EL REGISTRO DE LOS PROPONENTES: 2025/04/09

De acuerdo a la evaluación del comité económico, se concluye que los oferentes **HIGH TECH SERVICES CORP** y **REALTIME CONSULTING & SERVICES SAS** podrán subsanar los documentos anteriormente requeridos en los términos del cronograma del presente proceso, a través de la plataforma SECOP II.

COMITÉ JURÍDICO: mediante comunicación oficial GS-2026-016369-DIPOL del 23/04/2026, presentó la siguiente respuesta:

ÍTEM	ASPECTOS A EVALUAR	OFERENTE	OFERENTE
	Documentos de Orden Jurídico 1.2	**REALTIME CONSULTING & SERVICES S.A.S**	**HIGH TECH SERVICES CORP (HTS CORP)**
1.2.1	Carta de presentación de la oferta formulario No 1.	CUMPLE	CUMPLE
1.2.2	Fotocopia de cédula del representante legal	CUMPLE	CUMPLE
1.2.3	Certificado de Contraloría	CUMPLE	CUMPLE
	Certificado de Procuraduría	CUMPLE	CUMPLE
	Antecedentes Judiciales de Policía Nacional	CUMPLE	CUMPLE
	Inhabilidades Ley 1918 de 2018	CUMPLE	CUMPLE
	Sistema Registro Nacional de Medidas Correctivas	CUMPLE	CUMPLE
1.2.4	Certificado de Registro Único Tributario	CUMPLE	CUMPLE
1.2.5	Certificación expedida por revisor fiscal o declaración juramentada en caso de personal natural o del representante legal del proponente, señalando para el primero el número de la tarjeta profesional y anexando fotocopia de la misma. Si es persona natural, declaración juramentada, en la cual certifique el pago de seguridad social (salud, pensión y riesgos profesionales); y si tiene empleados a su cargo certificar el pago de los aportes parafiscales de sus empleados, indicando que se encuentra al día con dichos pagos (caja de compensación familiar, SENA e instituto colombiano de bienestar familiar). desarrollo del presente numeral se entiende suministrada bajo gravedad de juramento, respecto su fidelidad y veracidad.	CUMPLE	CUMPLE
1.2.6	Compromiso anticorrupción formulario No. 3	CUMPLE	CUMPLE
1.2.7	Compromiso de confidencialidad formulario No. 4	CUMPLE	CUMPLE
1.2.8	Formulario No. 5 SGSST	CUMPLE	CUMPLE
1.2.9	Garantía de seriedad de la oferta por el 10% y cubrir a partir de la fecha de presentación de la oferta y cuatro (4) meses más, expedida a favor de la dirección de inteligencia policial NIT 830.000.097-5 – AV. Boyacá 142a-55 – teléfono 5189223.	CUMPLE	CUMPLE
1.2.10	Certificado de Existencia y Representación Legal vigente, renovada la matricula mercantil para el año 2026. De igual forma, allegar el registro único de proponentes, tener en cuenta que de acuerdo con lo señalado en el artículo 2.2.1.1.1.5.1. del Decreto 1082 de 2015, la renovación de este registro debe realizarse entre el 1.º de enero y a más tardar el quinto (5) día hábil del mes de abril de cada año. De lo contrario, cesarán los efectos, no podrán renovar certificado y deberán realizar una nueva inscripción.	**NO CUMPLE**	**NO CUMPLE**
1.2.11	Verificar que la persona natural o el representante legal de la persona jurídica, no este reportado ante el REDAM Certificación expedida por MINTIC	CUMPLE	CUMPLE
1.2.13	Formato no. 2 inhabilidades e incompatibilidades	**NO CUMPLE**	CUMPLE

RESUMEN DE LA EVALUACIÓN JURÍDICA

1. REALTIME CONSULTING & SERVICES S.A.S.: **NO CUMPLE** con el requisito jurídico habilitante **1.2.10.**, teniendo en cuenta que allegó soporte documental parcial, ya que al verificar no aportó el ***"CERTIFICADO DE INSCRIPCIÓN Y CLASIFICACIÓN REGISTRO ÚNICO DE PROPONENTES"***.

2. REALTIME CONSULTING & SERVICES S.A.S **NO CUMPLE** con el requisito jurídico habilitante **1.2.13.** formulario No. 2, inhabilidades e incompatibilidades, toda vez que no diligenció el documento conforme a lo estipulado por esta entidad.

Observaciones HIGH TECH SERVICES CORP (HTS CORP):

1. HIGH TECH SERVICES CORP (HTS CORP): **NO CUMPLE** con el requisito jurídico habilitante **1.2.10**. con respecto a *"**ALLEGAR EL REGISTRO ÚNICO DE PROPONENTES, TENER EN CUENTA QUE DE ACUERDO CON LO SEÑALADO EN EL ARTÍCULO 2.2.1.1.1.5.1. DEL DECRETO 1082 DE 2015, LA RENOVACIÓN DE ESTE REGISTRO DEBE REALIZARSE ENTRE EL 1° DE ENERO Y A MÁS TARDAR EL QUINTO (5) DÍA HÁBIL DEL MES DE ABRIL DE CADA AÑO**"*, toda vez que el documento presentado por el oferente no fue renovado.

Finalmente, este comité evaluador considera pertinente que le sea **REQUERIDO A LOS OFERENTES LA SUBSANACIÓN DE LOS REQUISITOS JURÍDICOS HABILITANTES**, dentro de los términos de ley establecidos en el pliego de condiciones.

En conclusión, y de acuerdo a lo manifestado por los comité técnico, jurídico y económico los oferentes **HIGH TECH SERVICES CORP** y **REALTIME CONSULTING & SERVICES SAS** podrán subsanar los diferentes requisitos exigidos dentro de los términos de ley establecidos en el pliego de condiciones del proceso PN DIPOL SA 020-2026.

Atentamente,

Capitán **ALDEMAR ANDRÉS OSPINA MORALES**
Jefe Grupo Investigación, Innovación y Analítica de Datos

Anexos: tres (comunicación oficial GS-2026-016481-DIPOL en 12 folios, comunicación oficial GS-2026-016147-DIPOL en un folio y comunicación oficial GS-2026-016369-DIPOL en dos folios)

Elaboró: CT. ALDEMAR ANDRÉS OSPINA MORALES
DIPOL - GRIAN

Revisó: CT. ALDEMAR ANDRÉS OSPINA MORALES
DIPOL - GRIAN

Fecha de elaboración: 24/04/2026
Ubicación: \\192.168.211.250\datos\2026\PROCESOS CONTRACTUALES\GERENTE\PN DIPOL SA 020-2026

Avenida Boyacá 142ª 55
Teléfono: 5189271
dipol.grian@dipol.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE INTELIGENCIA POLICIAL
GRUPO TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

GS-2026- 016481 **/ DIPOL – GUTIC – 20.1**

Bogotá D.C., 23 de abril de 2026

Señor capitán
ALDEMAR ANDRÉS OSPINA MORALES
Gerente invitación PN DIPOL SA 020-2026
Avenida Boyacá 142A – 55
Bogotá D.C.

Asunto: evaluación técnica proceso PN DIPOL SA 020-2026

Respetuosamente me permito enviar a mi capitán, la evaluación técnica de las ofertas de las empresas **REALTIME CONSULTING & SERVICES S.A.S y HIGH TECH SERVICES CORP (HTS CORP) S.A.S.**, dentro del proceso PN DIPOL SA 020-2026, cuyo objeto es "ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL", así:

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
1.	**GENERALES**				
1.1	La adquisición del licenciamiento para la solución tecnológica de protección de correo electrónico y herramientas de colaboración en la nube deberá permitir la conexión y gestión de 400 cuentas de correo.	**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
1.2	**MARCA:** la que indique el oferente **REFERENCIA:** la que indique el oferente **FABRICANTE:** la que indique el oferente		**X**	**X** Trend AI TREND VISION ONE Trend Micro Incorporated	
2.	**PROTECCIÓN DE CORREO**				
2.1	La solución deberá tener la capacidad para proteger correos internos de la organización que provengan de la plataforma de Microsoft Office 365		**X**	**X**	
2.2	La solución deberá tener la capacidad para proteger correos en la plataforma Microsoft Office 365 de dominio externos y ajenos a la empresa		**X**	**X**	
2.3	La solución deberá tener motores para la detección de malware con la capacidad de identificar Exploits en documentos y archivos de Office.		**X**	**X**	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
2.4	La solución deberá tener Sandbox para análisis de amenazas desconocidas y ataques de día cero.		X	X	
2.5	La solución deberá ofrecer un análisis de riesgo para reducir el impacto en los usuarios		X	X	
2.6	La solución deberá tener escaneo de URL en el cuerpo de los correos y en los archivos adjuntos.		X		X
2.7	La solución deberá ofrecer protección avanzada contra amenazas para OneDrive, SharePoint, Teams.		X		X
2.8	La solución debe tener una capacidad de protección colaborativa para detectar archivos maliciosos que se encuentran en SharePoint, OneDrive, Teams.		X		X
2.9	La solución deberá tener plantillas personalizables de DLP para controlar la fuga de información permitiendo realizar pruebas de expresiones regulares y listados de palabras para nuevas plantillas		X		X
2.10	La solución deberá tener DLP a nivel de Email con la capacidad de descubrir y reportar violaciones a las políticas.		X		X
2.11	La solución deberá tener DLP a nivel de SharePoint, Teams y One Drive, con la capacidad de descubrir y reportar violaciones a las políticas.		X		X
2.12	La solución deberá ofrecer disponibilidad del servicio superior a >99%.		X		X
2.13	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 (Limpiar, Eliminar, Tag, encriptar, notificar).		X		X
2.14	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.		X		X
2.15	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.		X		X
2.16	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 dé clic en el enlace		X		X
2.17	La solución deberá tener la capacidad en la consola en la nube de reportar ataques dirigidos.		X	X	
2.18	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.		X	X	
2.19	La solución debe proporcionar seguridad para la información que se encuentra almacenada en la nube y garantizar la privacidad de la misma.		X		X
2.20	La solución debe tener la capacidad de identificar amenazas que aún no han sido reportadas con el análisis de los archivos.		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
2.21	La solución debe proporcionar protección contra ataques de BEC (Business Email Compromise – Compromiso en cuentas corporativas) con el análisis de los mensajes.		X	X	
2.22	La solución debe contar con la capacidad de detectar el análisis de estilo de escritura impulsado por la IA embebida en la solución de los usuarios de alto perfil para detectar ataques BEC		X	X	
2.23	La solución debe contar con la capacidad de tener una funcionalidad de inteligencia correlacionada		X	X	
2.24	La solución debe contar con la capacidad de detectar posando el mouse en las url's adjuntas al correo, según a nivel reputacional y bloquear el acceso a determinado sitio web, cuando el mismo infrinja la reputación		X	X	
2.25	La solución debe tener la capacidad de detectar ataques dirigidos mediante explotación de archivos.		X	X	
2.26	La solución debe tener la capacidad de realizar un análisis avanzado de los archivos usando Machine Learning, para identificar amenazas que aún no han sido reportadas, pero que pueden generar una afectación sobre los datos o el sistema que está utilizando el usuario.		X	X	
2.27	La solución debe tener la capacidad de brindar protección contra ataques avanzados como Business Email Compromise (BEC), Ramsomware, Phishing avanzado entre otros ya sea mediante firmas anti-spam o reglas heurísticas.		X	X	
2.28	La solución debe tener la capacidad de tomar una acción 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.		X		X
2.29	La solución debe tener la capacidad de tomar una acción 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.		X		X
2.30	La solución debe tener la capacidad de tomar una acción sobre los archivos localizados en el servicio Sharepoint, Teams, One Drive y que sean analizados con el sandbox e identificados como maliciosos o sospechosos, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una descripción en el correo para informar al usuario por que el correo ha sido enviado a cuarentena o eliminados.		X	X	
2.31	La solución debe tener la capacidad de notificar al usuario cuando algún correo que iba dirigido a tuvo alguna acción reactiva, basado en las reglas configuradas, dicha notificación debe indicarle que acción se tomó sobre el correo que iba dirigido a él y la razón de esta.		X		X

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
2.32	La solución debe tener la capacidad de sincronizarse y actualizar la lista de objetos sospechosos cuando se existe la integración con la consola de gestión.		X		X
2.33	La solución debe tener la capacidad de integrarse con el Active Directory Federation Services o Microsoft Azure AD, para permitir agregar usuarios administradores locales que puedan administrar la consola usando las credenciales registradas en estos servicios		X	X	
2.34	La solución debe contar con la capacidad de tener una funcionalidad para gestionar integraciones de tecnologías de terceros como Firewalls Fortinet, Palo Alto, SIEM Qradar y Directorio Activo On-Premise y opcionalmente con Gestores de vulnerabilidades, Proveedores de nube, Dominios, para enviar información hacia las determinadas fuentes o en algunos casos, recibir información de estas para alimentar la postura de riesgo de la compañía.		X	X	
2.35	La solución debe permitir a los administradores configurar la lista de excepciones, de los archivos detectados mediante Machine Learning como maliciosos o sospechosos.		X		X
2.36	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 prevención de filtración de datos de la organización.		X	X	
2.37	La solución debe permitir realizar un escaneo manual en modo de evaluación para permitir a los administradores verificar las reglas que serán aplicadas para proteger Office 365 sin tomar ninguna acción sobre dichos correos o archivos.		X	X	
2.38	La solución debe tener una tecnología de reputación web para escanear URL en mensajes de correo electrónico y rastrear la credibilidad de los dominios web asignando un puntaje de reputación basado en factores que incluyen la antigüedad del sitio web, cambios históricos de ubicación e indicaciones de actividades sospechosas descubiertas a través del análisis del comportamiento de malware, como ataques de phishing que están diseñados para engañar a los usuarios para que proporcionen información personal.		X	X	
2.39	La solución debe soportar la extracción de URL de códigos QR para detener ataques de phishing, ransomware y BEC.		X	X	
2.40	La solución debe soportar el escaneo dinámico de URL y rastrear las páginas web de URL no probadas en tiempo real para determinar si las páginas contienen patrones maliciosos para proteger a los usuarios de ataques de phishing de día cero.		X	X	
2.41	La solución debe aprovechar la visión computacional basada en inteligencia artificial (IA) para analizar elementos de sitios web de marca y reconocer sitios falsos para proteger a los usuarios contra el phishing de credenciales.		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
2.42	La visión artificial basada en IA debe poder reconocer elementos clave de una página o formularios de inicio de sesión de un servicio en la nube válidos para ayudar a evitar que los usuarios envíen credenciales a sitios no confiables y ayudarlos a deshacerse de la vulneración de la cuenta.		X		X
2.43	La solución debe ofrecer capacidad de prevención de pérdida de datos (DLP) tanto para mensajes de correo electrónico como para archivos en servicios de colaboración en la nube.		X	X	
2.44	La solución debe ofrecer la correlación de datos de correo electrónico XDR entre capas o más allá con identidad, punto final, red y otros vectores.		X	X	
2.45	La solución debe incluir modelos de detección predefinidos que combinen múltiples reglas y filtros que utilicen técnicas como el aprendizaje automático y el apilamiento de datos. Debe actualizarse periódicamente para mejorar la detección de amenazas y reducir las alertas de falsos positivos.		X	X	
2.46	La solución debe tener la capacidad de habilitar o deshabilitar modelos de detección y agregar y configurar excepciones de modelos de detección según los requisitos de la organización.		X	X	
2.47	La solución debe permitir la creación de modelos de detección personalizados y filtros de eventos personalizados que definan los eventos que el modelo utiliza para activar alertas.		X	X	
2.48	La solución debe poder analizar y determinar si ciertos indicadores señalan un ataque en curso, lo que permitirá al equipo SOC tomar medidas oportunas de prevención, investigación y mitigación contra campañas de ataques específicos.		X	X	
2.49	La solución debe enumerar todos los eventos asignados al marco MITRE ATT&CK; con el fin de que el analista SOC puede usar estos eventos como punto de partida para realizar investigaciones adicionales.		X	X	
2.50	La solución debería proporcionar más contexto con mapeo a los TTP (Técnicas, Tácticas y Procedimientos) MITRE ATT&CK para una detección más rápida y alertas de mayor fidelidad.		X	X	
2.51	La solución debe tener la capacidad de escribir consultas de búsqueda personalizadas, agregar las consultas guardadas a la lista de seguimiento y ejecutarlas automáticamente contra los últimos datos de telemetría en un intervalo.		X	X	
3.	**ADMINISTRACIÓN**				
3.1	La solución debe ser compatible con el acceso basado en roles (RBAC) para la administración de derechos de acceso a la consola		X	X	
3.2	La solución puede distinguir el acceso a funciones y parámetros según los roles.		X	X	
4.	**ALERTAS**				
4.1	La solución debe poder notificar a un administrador en función de un umbral personalizado con el fin de evitar fatigas de alertas		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
4.2	La solución debe poder notificar a un destinatario interno en caso de correo electrónico en cuarentena / eliminado / limpiado		X	X	
4.3	La solución debe poder enviar eventos de alerta por correo electrónico al SIEM QRadar		X	X	
5.	**REPORTES**				
5.1	La solución debe conservar los registros (usuario y administrador) durante al menos 3 meses		X	X	
5.2	La solución debe poder mostrar el panel del día, la semana o el mes actual con: 1.El número de correos electrónicos analizados, no analizados, sospechosos, bloqueados, en cuarentena. 2. El tiempo promedio de escaneo, particularmente en el tiempo de análisis de sandboxing. 3. El nivel de riesgo de los correos electrónicos sospechosos. 4. El top 10 de malware detectado. 5. El top 10 de buzones con actividad sospechosa.		X	X	
6.	**CAPACIDADES DE DETECCIÓN Y RESPUESTA EN OFFICE 365 PARA LA ATENCIÓN DE INCIDENTES**				
6.1	Extended Detection and Response (XDR) debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.		X	X	
6.2	Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis entre ellas Data Stacking y Machine Learning.		X	X	
6.3	La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.		X	X	
6.4	La solución deberá contar con una interfaz visual de correlación e investigación que centralice, agrupe y correlacione automáticamente los eventos de seguridad, utilizando capacidades de inteligencia artificial, enriquecida con inteligencia de amenazas y alineada con las tácticas y técnicas del marco MITRE ATT&CK, permitiendo visualizar de forma gráfica el linaje de los eventos, las comunicaciones de red y el impacto sobre los activos comprometidos.		X	X	
6.5	Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.		X	X	
6.6	Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).		X	X	
6.7	Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.		X	X	
6.8	XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.		X	X	
6.9	Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz para ver las accionas que una amenaza llevó a cabo en un correo de Office 365		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
6.10	Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el fabricante		X	X	
6.11	La capacidad de Inteligencia de Amenazas (Threat Intelligence) embebida debe ser capaz de identificar la campaña asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.		X	X	
6.12	La solución debe tener un chatbot impulsado por IA para guiar las investigaciones y brindar respuestas automáticas a cualquier pregunta relacionada con la ciberseguridad.		X	X	
6.13	La solución debe tener la capacidad de agregar o eliminar indicadores de compromiso admitidos a la lista de bloqueo, incluidos, entre otros, hash de archivo, URL, dirección IP y dominios.		X	X	
6.14	La solución debe ofrecer un enfoque holístico a la seguridad del correo electrónico con protección diseñada específicamente para aplicaciones de correo electrónico y colaboración, y enriquecida con XDR y capacidades de gestión de exposición al riesgo cibernético.		X		X
6.15	La solución debería tener la capacidad de mover el mensaje de correo electrónico seleccionado a la carpeta de cuarentena y poner en cuarentena el mensaje de todos los buzones afectados.		X	X	
6.16	La solución debería tener la capacidad de eliminar el mensaje de correo electrónico seleccionado de los buzones seleccionados.		X	X	
6.17	La consola debe proporcionar diferentes métodos de búsqueda, filtros y un lenguaje de consulta fácil de usar para identificar, categorizar y recuperar resultados de búsqueda.		X	X	
7.	**GESTIÓN DE MODELOS DE DETECCIÓN**				
7.1	Los modelos de detección deben consistir en uno o más conjuntos de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK		X	X	
7.2	El fabricante debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos.		X	X	
7.3	Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).		X	X	
7.4	La solución deberá permitir a los administradores habilitar, deshabilitar y ajustar la sensibilidad de los modelos de detección, así como configurar de manera granular los criterios de envío de alertas hacia la consola de investigación y correlación, basándose en niveles de severidad, categorías de amenaza y grado de confianza del modelo, con el objetivo de optimizar los tiempos de detección y respuesta del equipo de seguridad.		X		X
7.5	Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE.		X		X

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	Critico: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. Alto: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medio: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Bajo: Hay indicadores levemente sospechosos. Usado para monitoreo y caza de amenazas (Threat Hunting).				
7.6	Los modelos deben especificar y permitir modificar el estado: encendido/apagado		X	X	
7.7	Los modelos deben especificar la última vez que se actualizó		X	X	
8.	**AUTOMATIZACIÓN**				
8.1	La solución debe contar con la capacidad de enviar alertas por medio de la integración de webhooks. Las alertas deberán ser configurables por nivel de severidad, permitiendo que solo las alertas clasificadas como 'altas' o 'críticas' sean enviadas, mientras que las alertas informativas se mantengan exclusivamente en la consola central.		X	X	
8.2	La solución debe contar con la capacidad de generar una serie de flujo de procesos que permita tomar acciones de respuesta automatizadas por medio de las fuentes propias o Tecnologías de tercero que permitan dependiendo de la capa de seguridad tomar una acción de respuesta, para el caso de correo e identidad, mandar a cuarentena el mensaje, o forzar a cerrar sesión a la identidad, forzar a reiniciar la contraseña, entre otros.		X	X	
9.	**ADMINISTRACIÓN**				
9.1	La configuración administrativa de XDR debe brindar a los usuarios la capacidad de configurar cuentas de usuario, roles y configuraciones, conectar productos adicionales y configurar opciones de monitoreo adicionales. Las siguientes opciones deben estar disponibles:		X	X	
9.2	**1.** SAML Single Sign-On: Debe soportar inicio de sesión SAML, single sign-on (SSO) utilizando las credenciales corporativas. **2.** Gestión de Cuenta: Debe permitir crear usuarios locales y usuarios para aplicaciones de terceros que se conectan a la API. **3.** Gestión de Role: Debe permitir ver y configurar el acceso basado en roles que se aplican a los usuarios aplicativos de terceros que se conectan a través de la API **4.** Conector de Producto: Debe permitir conectar de manera nativa el correo, y de manera alternativa los puntos finales, servidores, Nube, y productos de red. **5.** Logs de Auditoria: Debe proveer logs de auditoría que provee un resumen de acceso de usuario, acciones relacionadas con las Apps, cambio de		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	configuraciones, y otras modificaciones que ocurran usando la consola XDR o las APIs. **6.** Soporte Remoto: debe permitir a los ingenieros de Soporte acceder a la consola de XDR para resolución de problemas y recolección de "debug logs" si es necesario.				
10.	**GESTÓN Y OPERACIÓN**				
10.1	La solución debe poder consolidar la protección de correo electrónico SaaS, local, de puerta de enlace y API en una única plataforma integrada.		X	X	
10.2	La solución debe proporcionar una plataforma centralizada de visibilidad y gestión en soluciones de correo electrónico basadas en API y gateway.		X		X
10.3	La solución debe proporcionar un inventario de activos de correo electrónico y poder mostrar los activos de correo electrónico de la organización, incluidas todas las cuentas de correo electrónico y todas las cuentas de dominio		X	X	
10.4	Debe poder identificar a los usuarios más específicos de la organización y configurar políticas de acceso condicional para los usuarios riesgosos.		X	X	
10.5	La solución debe tener la capacidad de automatizar una variedad de acciones utilizando manuales de seguridad para ayudar a reducir la carga de trabajo y acelerar las tareas de seguridad y las investigaciones.		X		X
10.6	La solución debe poder descifrar y escanear mensajes de correo electrónico y archivos adjuntos cifrados con MIP en Exchange Online y archivos cifrados con MIP en SharePoint, OneDrive y MS Teams.		X	X	
10.7	La solución debe tener un panel altamente personalizable que proporcione widgets que muestren estadísticas de superficie de ataque, correo electrónico, identidad, entre otros.		X	X	
10.8	La solución debe ofrecer una integración de detección y respuesta de correo electrónico (Email DR) y Gestión de exposición de Riesgos		X	X	
10.9	La solución debe poder mostrar el mapeo MITRE ATT&CK de las tácticas y técnicas detectadas en la organización para las siguientes matrices MITRE ATT&CK. Empresa (Enterprise) Móvil (Mobile) ICS		X	X	
11.	**REQUERIMIENTOS DE LA PLATAFORMA**				
11.1	La solución debe proporcionar una plataforma unificada que permita a los equipos de seguridad ejecutar un análisis de causa raíz, investigar el perfil de ejecución de un ataque e identificar el alcance del impacto en los activos.		X	X	
11.2	La solución debe incluir un período estándar de retención de Alertas de Investigación y Correlación y registros de detección y actividad presentada en la funcionalidad de Correo y aplicaciones de colaboración, no menor a 180 días.		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
11.3	La solución debería ofrecer una opción para ampliar la retención de datos hasta 365 días.		X	X	
11.4	El fabricante deberá estar certificado con las siguientes normas internacionales de cumplimiento las cuales a su vez deberán dar alcance a la solución de seguridad a licenciar: ISO 27001 (Para lo cual se deberá anexar soporte directo firmado por ente certificador) ISO 27014 (Para lo cual se deberá anexar soporte directo firmado por ente certificador) ISO 27017 (Para lo cual se deberá anexar soporte directo firmado por ente certificador) SOC 2 o SOC 3 (la Entidad aceptará la entrega de "Bridge Letters" (Cartas de Continuidad) o documentos equivalentes emitidos por el fabricante o su firma auditora, siempre que estos certifiquen que el entorno de control de la solución no ha sufrido cambios significativos desde el último periodo de auditoría, garantizando así la idoneidad técnica durante todo el proceso de contratación)		X No anexo soportes solicitados	X CERTIFICACION ISO - 27001-27014-27034 certificate.pdf en-globalCERTIFICACION ISO - 27017-certificate.pdf SOC2_Bridge_Letter_Apr_2026.pdf	
12. INTEGRACIÓN CON TERCEROS Y API					
12.1	La solución debe poder integrarse con la funcionalidad de Protección de Información de Microsoft (MIP) para descifrar y escanear correos electrónicos y archivos cifrados con MIP.		X	X	
12.2	La solución debe poder integrarse con productos SIEM y SOAR comunes.		X	X	
12.3	La solución debe poder integrarse con soluciones IdP de terceros para los requisitos de inicio de sesión único (SSO).		X	X	
12.4	La solución debería poder generar claves API mediante control de acceso basado en roles para permisos más granulares. Las claves API deberían poder caducar y desactivarse desde la consola de administración.		X	X	
12.5	La solución también debe tener la capacidad de integrarse con otras soluciones de terceros a través de API.		X	X	
12.6	La solución debe proporcionar conectores listos para integrarse con otras soluciones de seguridad de terceros compatibles		X	X	
12.7	La solución debe ser integrable con al menos una solución de terceros de la siguiente categoría: Firewall Fortinet Firewall Paloalto SIEM QRadar Directorio Activo		X	X	
13. GESTIÓN DEL RIESGO					

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
13.1	El contratista debe ofrecer una solución que realice un análisis continuo y en tiempo real de todos los activos de la organización especialmente del correo electrónico, permitiendo una visión integral del riesgo de ciberseguridad. Se requiere: 1. Correlación unificada de telemetría desde múltiples fuentes. 2. Evaluación integral de riesgos. 3. Visibilidad de la superficie de ataque, incluyendo activos expuestos a Internet. 4. Puntuación de riesgo contextualizada, considerando la criticidad y la exposición de los activos.		X	X	
13.2	La solución debe contar con capacidades de inteligencia de amenazas en tiempo real para prevenir, detectar y priorizar vulnerabilidades críticas antes de que sean explotadas. Se requiere: 1. Integración con una iniciativa global de Zero Day (ZDI) para la detección temprana de vulnerabilidades. 2. Priorización basada en explotación activa en el mundo real, no solo en criticidad teórica. 3. Correlación automática con intentos de explotación detectados 4. Análisis de configuraciones incorrectas en múltiples plataformas.		X	X	
13.3	El contratista debe ofrecer una solución que permita actuar sobre los riesgos detectados sin intervención manual, asegurando una reducción proactiva de la superficie de ataque. Se requiere: 1. Recomendaciones accionables para mitigación inmediata de riesgos. 2. Playbooks de respuesta automatizados para la remediación de vulnerabilidades. 3. Integración con soluciones de control de acceso para respuesta automática ante amenazas. 4. Capacidad de personalización de reglas de riesgo. 5. Métricas de mejora de postura de seguridad en el tiempo.		X	X	
13.4	La plataforma debe proporcionar una vista centralizada del riesgo organizacional con métricas claras y accionables para la toma de decisiones estratégicas. Se requiere: 1. Vista unificada de los riesgos de la organización, sin necesidad de múltiples herramientas. 2. Métricas comparativas con la industria, permitiendo evaluar el nivel de seguridad frente a otros sectores. 3. Seguimiento de tendencias de riesgo en tiempo real. 4. KPIs de reducción de riesgo, con mediciones tangibles de mejora de seguridad. 5. Visualización dinámica de la superficie de ataque, permitiendo identificar activos críticos expuestos.		X	X	
13.5	El contratista debe garantizar que se cuente con capacidades avanzadas de análisis de riesgos en múltiples capas de seguridad. Se requiere:		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	1. Evaluación de riesgos en buzones de correo en la nube, detectando configuraciones inseguras o accesos sospechosos. 2. Detección de anomalías en comportamiento de usuarios, identificando accesos o actividades fuera del patrón normal.				
13.6	La solución debe poder gestionar todos los activos descubiertos desde una única consola de gestión unificada.		X	X	
13.7	La solución debe poder integrarse con proveedores externos para incorporar o enriquecer datos de la superficie de ataque.		X	X	
13.8	La solución debe contar con la capacidad de tener embebido un apartado para identificar la postura de identidad a través de la integración con el AD, generando un índice numérico de riesgo que permita identificar cuáles usuarios tiene MFA deshabilitado, contraseña no robusta, política de expiración de contraseña deshabilitado, y eventos de riesgo (Viajes imposibles, volcado de credenciales, credenciales filtradas a la dark web, ataque de fuerza bruta, etc).		X	X	
13.9	La solución debe contar con la capacidad de tener una funcionalidad para realizar barridos de indicadores de compromiso (IOC's) basado en más de 30.000 reportes de la marca y fuentes de terceros (Entidades gubernamentales, centros de investigación, etc.) para confirmar si hay alguna amenaza en el ambiente que se empareje con estos reportes, y poder identificar el activo afectado.		X	X	
13.10	La solución debe ser capaz de identificar si la organización está por encima, por debajo o en promedio del nivel de riesgo de compañía a nivel de sector industrial, tamaño organizacional o regional.		X	X	
13.11	La solución debe ser capaz de modificar la criticidad de un activo en función de la necesidad de la compañía.		X	X	
13.12	La solución debe tener soporte integrado para manuales de seguridad que puedan usarse para la remediación automatizada.		X	X	
13.13	La solución debe poder evaluar la situación de seguridad de Internet y otros activos externos de la organización (Gestión de la superficie de ataque externa).		X	X	
13.14	La solución debe proporcionar una puntuación de riesgo para toda la organización basada en una evaluación continua de los riesgos en la organización.		X	X	
13.15	Incorpore la criticidad de los activos, las vulnerabilidades, la actividad de amenazas y la configuración de los controles de seguridad en el cálculo del puntaje de riesgo para cada tipo de activo.		X	X	
13.16	La solución debe proporcionar un índice de exposición que resuma la probabilidad de que se produzca una vulnerabilidad o amenaza en el entorno.		X	X	
13.17	Debe utilizar múltiples proveedores de datos de descubrimiento (la dependencia del agente existente		X	X	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	debe complementarse con proveedores de descubrimiento adicionales).				
13.18	La solución debe proporcionar métricas de gestión de vulnerabilidades para activos internos y de acceso a Internet a lo largo del tiempo y permite comparar la puntuación de las organizaciones con el promedio global. Métrica: CVE únicos altamente explotables.		X	X	
13.19	La solución debe proporcionar métricas de gestión de vulnerabilidades para activos internos y de Internet a lo largo del tiempo y permite comparar la puntuación de las organizaciones con el promedio global. Métrica: Tiempo promedio sin parches.		X		X
13.20	La solución debe proporcionar la función de poder identificar aquellos riesgos de mayor prioridad para mitigar basado en la meta que el cliente desee abordar para disminuir el número de riesgo, y así, la solución deba calcular basado en la métrica ingresada por el cliente, lograr mostrarte los riesgos de mayor foco a mitigar.		X		X
13.21	Debe proporcionar información sobre la postura de seguridad de la organización mediante un panel de control de nivel ejecutivo. Debe poder mostrar la puntuación de riesgo general de la empresa, los riesgos de los activos individuales, una vista de los ataques en curso y sus factores de riesgo contribuyentes.		X		X
13.22	Los informes se pueden generar por demanda o mediante programación.		X	X	
13.23	El contenido de los informes se puede filtrar para limitar la salida según criterios seleccionados		X	X	
13.24	Debe proporcionar la capacidad de la vista de inventario y de operaciones tener la facilidad de realizar filtros por diferentes tipos de información (Tipo de Activo, qué tecnología lo descubrió, índice de riesgo, etc).		X	X	
13.25	La solución debe ser considerada líder en el segmento de gestión de exposición de ciber-riesgos por alguna firma global reconocida en investigación y consultoría en tecnología de la información.		X	X	
14. SOPORTE DEL FABRICANTE					
14.1	El fabricante como mínimo debe: • Brindar soporte telefónico y basado en la web • Permitir la generación de casos a través del teléfono y del portal de soporte las 24 horas del día, los 7 días de la semana • brinda soporte técnico las 24 horas para problemas urgentes (críticos), mientras que las consultas y problemas no críticos deben ser atendidos durante el horario comercial habitual • Soportar la instalación y actualización de productos • brindar transferencia de conocimiento para mínimo 4 personas por 20 horas y acceso a base de conocimientos (*knowledge base*) y mejores prácticas	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	• Análisis de archivos sospechosos • Actualizaciones y mejoras de la solución				
15.	**TIEMPOS DE RESPUESTA Y SEVERIDAD**				
15.1	El fabricante como mínimo debe cumplir con: Severidad 1 (Crítica): Dentro de 1 hora. Se aplica cuando los componentes principales del producto quedan inoperables, hay un impacto crítico en las operaciones del negocio y no existe una solución alternativa (workaround). ◦ Nota: Debe enviarse por teléfono (o en línea seguido inmediatamente de una llamada). • Severidad 2 (Alta): Dentro de 4 horas hábiles locales. Se aplica cuando los componentes principales están severamente deteriorados o degradados, causando un impacto significativo en las operaciones comerciales. • Severidad 3 (Media): Dentro de 1 día hábil local. Se aplica cuando la funcionalidad del producto está afectada pero operativa, o hay fallos en componentes no esenciales. El impacto en el negocio es medio o bajo y existe una solución alternativa. • Severidad 4 (Baja): Dentro de 2 días hábiles locales. Se utiliza para problemas leves, solicitudes de mejoras, preguntas generales o incidentes con poco o nulo impacto en la DIPOL	**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
16.	**NIVEL DE EDUCACION O NIVEL ACADEMICO**				
16.1	Un profesional Ingeniero Electrónico, de Sistemas o Telecomunicaciones, con mínimo 2 años de experiencia contada a partir de la expedición de la tarjeta profesional, este se deberá acreditar anexando a la propuesta acta de grado y diploma con su tarjeta profesional vigente. Dentro de los dos años de experiencia se debe acreditar experiencia de seis (6) meses, en configuración y mantenimiento en soluciones de seguridad informática la cual se acreditará anexando certificación firmada por el oferente o el fabricante, y Especialización en Seguridad de la Información o Informática la cual se acreditará anexando acta de grado y diploma. Certificaciones Mínimas: - Profesional certificado por el fabricante de la solución ofertada, con certificación vigente de nivel avanzado (Advanced) en la herramienta solicitada. (anexar certificación) - CEH (Certified Ethical Hacker) vigente (anexar certificación) - CISP- Certified Information Security Professional (anexar certificación) **Nota:** para personal que haya obtenido su título por fuera del país, tendrá que demostrar la convalidación de este ante el Ministerio de Educación, teniendo en cuenta la Ley 842 de 2003 Articulo 6 y la Circular		**X** No se evidencia que se relacione en la propuesta el personal solicitado		**X**

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	Externa Única de Colombia Compra Eficiente, Ítem 9.3 Acreditación de la formación académica.				
16.2	Un profesional Ingeniero electrónico, de sistemas o Telecomunicaciones, este se deberá acreditar anexando a la propuesta acta de grado y diploma con su tarjeta profesional vigente. Este profesional deberá contar con Magister en Ciberseguridad y Ciberdefensa que deberá ser acreditado anexando acta de grado y diploma. Este profesional deberá contar con mínimo 3 años de experiencia contada a partir de la expedición de la tarjeta profesional. Adicionalmente el oferente o fabricante deberá certificar experiencia de este profesional gerenciando proyectos de Ciberseguridad. Certificaciones mínimas - Project Management Professional – PMP (anexar certificado) - Scrum Master Professional Cerfificate (anexar certificado) - **Nota:** para personal que haya obtenido su título por fuera del país, tendrá que demostrar la convalidación de este ante el Ministerio de Educación, teniendo en cuenta la Ley 842 de 2003 Articulo 6 y la Circular Externa Única de Colombia Compra Eficiente, Ítem 9.3 Acreditación de la formación académica.		X No se evidencia que se relacione en la propuesta el personal solicitado	X JORGE HERNANDO PORRAS GONZALEZ ActaGrado - Ingeniero Sistemas. pdf DocumentosAcademicos.pdf Tarjeta o matricula profesional Jorge Porras.pdf ActaGrado MaestriCSCD.pdf Certificación Laboral Jorge Porras.pdf CertificacionPMP.pdf CertificacionesScrum.pdf	
16.3	Un Técnico o tecnólogo en sistemas, telecomunicaciones, electrónica o afines, este se acreditará anexando acta de grado y diploma. Deberá contar con mínimo dos años de experiencia en configuración y mantenimiento en soluciones de seguridad informática. Certificaciones Mínimas: - Profesional certificado por el fabricante de la solución ofertada, con certificación vigente		X No se evidencia que se relacione en la propuesta el personal solicitado	X JORGE LUIS CEPEDA SANABRIA Diploma Tecnico.pdf Acta de grado	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	de nivel avanzado (Advanced) en la herramienta solicitada. (anexar certificación) - - **Nota:** para personal que haya obtenido su título por fuera del país, tendrá que demostrar la convalidación de este ante el Ministerio de Educación, teniendo en cuenta la Ley 842 de 2003 Articulo 6 y la Circular Externa Única de Colombia Compra Eficiente, Ítem 9.3 Acreditación de la formación académica.			Tecnico.pdf Certificacion Advanced email - Jorge Cepeda.jpeg	
17.	**CERTIFICACIONES ADICIONALES**				
17.1	Certificación de Partner en alguno de los dos niveles más altos, expedida por el fabricante de la solución propuesta no mayor a treinta (60) días anteriores al cierre del proceso, en la que conste que el proponente cuenta con la calidad de canal oficial y que certifique venta y distribución de la solución propuesta		**X** No se anexo certificación solicitada	**X** TM_17.2026_-_DIPOL_-_Carta_Partner_HIGH_TECH_SERVICES_.docx.pdf	
18.	**EXPERIENCIA**				
18.1	Con el fin de garantizar la calidad de los servicios a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en la clasificación 43222600 y/o 43222500 y/o 43233200 y/o 81112200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a superior a 158,66 S.M.M.L.V, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		**X** No anexo registro único de proponentes		**X** No tiene el RUP actualizado a la vigencia.
19.	**GARANTÍA TECNICA**				
19.1	El contratista frente a la celebración de contratos de software o licenciamiento, tendrá que entregar ***certificados de autenticidad, el certificado de distribuidor autorizado y las facturas***" los cuales deberán ser entregados durante la ejecución del contrato, previo acuerdo con el supervisor del mismo.	**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
19.2	El contrato tendrá su ejecución hasta el 10 agosto del 2026 y deberá contar con una garantía de treinta y tres (33) meses después de la finalización de su ejecución.	**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA		**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
		TECNICA PN DIPOL SA 020-2026 – I.pdf		PN DIPOL SA 020-2026 - I Copy.pdf	
19.3	El contratista deberá proporcionar soporte técnico durante los treinta y tres (33) meses siguientes a la finalización de la ejecución del contrato, atendiendo cualquier requerimiento formulado por los funcionarios de la DIPOL, así como los incidentes que afecten el normal funcionamiento de la plataforma poniendo a disposición el personal calificado y los recursos necesarios para su resolución conforme al alcance contractual; los casos reportados deberán ser atendidos en un tiempo de seis (6) horas y resueltos en un plazo máximo de veinticuatro (24) horas contadas a partir de su notificación. En los casos de requerirse aumentar este tiempo, se debe elaborar por parte de la empresa contratada un informe estableciendo el cronograma de respuesta y los motivos.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
19.4	En caso de presentarse indisponibilidad total del servicio durante el periodo de garantía, la empresa contratista deberá atender el soporte en sitio, en un tiempo de respuesta de máximo cuatro (4) horas, hasta restablecer el servicio.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
19.5	Durante el período de garantía, el contratista deberá realizar un mínimo de once (11) visitas de seguimiento, revisión, actualización u mejoras sobre el software que compone la solución de seguridad. Estas visitas deberán ser programadas según la necesidad y de común acuerdo con el administrador de la herramienta tecnológica en DIPOL, garantizando al menos una (1) visita trimestral.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20. SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO					
20.1	El oferente deberá entregar en la oferta el documento firmado por el representante legal el cual indique el número de trabajadores permanentes, el nivel de riesgo de su principal actividad económica y asimismo anexar la calificación de los estándares mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo de la vigencia anterior, lo anterior como consideración a la Resolución 0312 del 13 de febrero del 2019 del Ministerio de Trabajo "*Por la cual se definen los Estándares Mínimos del Sistema de*		X No anexo el documento solicitado.	X SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	Gestión de SST", en cumplimiento al art. 1 la presente Resolución tiene por objeto establecer los Estándares Mínimos del SG-SST para las personas naturales y jurídicas señaladas en el art. 2 aplica a los empleadores públicos y privados, a los contratantes del personal bajo modalidad de contrato civil, comercial o administrativo, a los trabajadores dependientes e independientes, a las organizaciones de economía solidaria y del sector cooperativo a las agremiaciones u asociaciones que afilian trabajadores independientes al sistema de seguridad social integral, a las empresas de servicios temporales, a los estudiantes afiliados al Sistema General de Riesgos Laborales y los trabajadores en misión; a las administradoras de riesgos laborales; a la Policía Nacional en lo que corresponde a su personal no uniformado y al personal civil de las Fuerzas Militares; quienes deben implementar los Estándares Mínimos del Sistema de Gestión de SST en el marco del Sistema de Garantía de Calidad del Sistema General de Riesgos Laborales.			TRABAJO .pdf	
20.2	El contratista deberá entregar al supervisor del contrato los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada.	**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.3	En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al supervisor del contrato, con el fin de que este haga llegar la copia al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución **1401** del **14/05/2007** del Ministerio de Trabajo y Protección Social "*Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo*" o cualquiera que la modifique, reemplace o sustituya.	**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.4	El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato.	**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-		**X** ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
		2026 – I.pdf		2026 - I Copy.pdf	
20.5	En caso de presentarse una emergencia dentro de las instalaciones durante el desarrollo del objeto contractual, el contratista deberá garantizar que el personal bajo su mando, atienda las recomendaciones durante la activación del plan de emergencia de las instalaciones policiales.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.6	En caso de que se desarrolle en la Dirección de Inteligencia Policial una auditoría del SG-SST durante la ejecución del contrato, el contratista deberá suministrar al supervisor del contrato la documentación requerida del objeto contractual.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
20.7	El contratista garantizará que el personal que ingrese a las instalaciones se encuentre con la debida identificación de la empresa.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
21. REQUERIMIENTOS AMBIENTALES					
21.1	El contratista deberá cumplir con la normatividad ambiental vigente nacional para reducir los aspectos e impactos ambientales asociados a la actividad y aplicación de buenas prácticas ambientales.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
21.2	Desarrollar y cumplir, durante la vigencia y ejecución del objeto del contrato, con las buenas prácticas ambientales con relación al ahorro y uso eficiente del	X ANEXO No. 2-8		X ANEXO No. 2-8	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	agua y la energía, así como el manejo integral de residuos (no peligrosos y peligrosos), establecidas por la Dirección y el marco del mantenimiento del Sistema de Gestión Ambiental en las instalaciones del contratante; que contribuyan al cumplimiento de la política ambiental y objetivos ambientales institucionales.	ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
	22. CUMPLIMIENTO CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN				
22.1	El contratista acatará los controles establecidos para la seguridad de la información en la Dirección de Inteligencia Policial, así como la firma del compromiso de reserva y la aplicación de los estudios de credibilidad y confiabilidad. Para ello el personal que realice la instalación o configuración, así como las actividades de soporte técnico de equipos y sistemas, deberá cumplir con un estudio de confiabilidad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato y el tiempo de la garantía técnica. En el evento de no aprobar dicho estudio algunas de las personas vinculadas a este proyecto, el contratista deberá realizar el cambio de estas personas por otras que también deberán cumplir con el estudio de confiabilidad requerido.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.2	Cláusula de Confidencialidad: Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el transcurso del proyecto, será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata, se considera también información confidencial: a) aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes. b) la que no sea de fácil acceso, y c) aquella información que no esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial, duración. El acuerdo regirá durante el tiempo que dure el proyecto, derechos de propiedad, toda información intercambiada es de propiedad exclusiva de la parte de donde proceda. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso, modificación o terminación. El acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.3	Confidencialidad e integridad de la información institucional: Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la preservación de la integridad y	X ANEXO No. 2-8 ESPECIFICACIONE		X ANEXO No. 2-8 ESPECIFICACIONE	

ÍTEM	DESCRIPCIÓN	REALTIME CONSULTING & SERVICES S.A.S		HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	
		CUMPLE	NO CUMPLE	CUMPLE	NO CUMPLE
	confidencialidad de la información institucional a la cual llegare a tener acceso directamente o por intermedio de terceros; en tal virtud, adoptará todas las medidas que sean necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida y suscribirá con la entidad los formatos de confidencialidad o reserva a que haya lugar por el termino establecido en la ley estatutaria 1621 de 2013.	S Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		S Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.4	En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del futuro contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de la labor. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información para lo cual deberá diligenciar el formulario establecido por la entidad contratante. El manejo de toda la información de arquitectura del sistema se considera CONFIDENCIAL, de manera que los planos, diseño, manuales técnicos y cualquier otro tipo de información estarán limitados únicamente a la interventora o supervisión. El suministro de copias para otras personas o entidades deberá ser solicitada a la DIRECCIÓN DE INTELIGENCIA DE LA POLICÍA NACIONAL.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.5	El contratista y todo el personal que realice la instalación y configuración de los equipos, cumplirá los protocolos descritos en el Manual del Sistema de Gestión de Seguridad de la Información de la Policía Nacional y el instructivo vigente mediante el cual se establece el Protocolo de Seguridad de la Información para el Servicio de Inteligencia Policial, debiendo suscribir el compromiso de reserva y el de confidencialidad.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	
22.6	Durante el desarrollo de la instalación y configuración, el contratista se compromete a no hacer uso indebido de las herramientas de software o hardware utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.	X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 – I.pdf		X ANEXO No. 2-8 ESPECIFICACIONES Y FICHA TECNICA PN DIPOL SA 020-2026 - I Copy.pdf	

Resumen de la evaluación REALTIME CONSULTING & SERVICES S.A.S:

La empresa REALTIME CONSULTING & SERVICES S.A.S, **NO CUMPLE** con todos los requisitos técnicos exigidos dentro del proceso PN DIPOL SA 020-2026, cuyo objeto es la "ADQUISICIÓN LICENCIAMIENTO

PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL", específicamente en los siguientes ítems del pliego de condiciones técnicas mínimas y ficha técnica:

Ítem 1.2 al ítem 11.3 y del ítem 12.1 al ítem 13.25: No se puede evaluar el cumplimiento de los anteriores ítems, toda vez, que no se especificó la marca, referencia y fabricante de la solución ofertada, sin poder establecer lo requerido en el anexo de especificaciones y ficha técnica.

Ítem 11.4: El oferente no anexó a su propuesta las certificaciones y documentos exigidos de las normas internacionales solicitadas.

Ítem 16.1 al ítem 16.3: El oferente no los documentos del personal que cumpla con los títulos y certificaciones exigidas.

Ítem 17.1.: El oferente no adjuntó la certificación de partner en los niveles requeridos, expedida por el fabricante de la solución ofertada.

Ítem 18.1.: El oferente no adjuntó el Registro Único de Proponentes (RUP).

Ítem 20.1.: El oferente no anexó los documentos exigidos en el presente proceso indicando el número de trabajadores permanentes, el nivel de riesgo de su principal actividad económica y asimismo no anexó la calificación de los estándares mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo de la vigencia anterior.

Resumen de la evaluación HIGH TECH SERVICES CORP (HTS CORP) S.A.S.:

La empresa HIGH TECH SERVICES CORP (HTS CORP) S.A.S., **NO CUMPLE** con todos los requisitos técnicos exigidos dentro del proceso PN DIPOL SA 020-2026, cuyo objeto es la "ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL", específicamente en los siguientes ítems del pliego de condiciones técnicas mínimas y ficha técnica:

Ítems 2.6 al 2.16, 2.19, 2.28, 2.29, 2.31, 2.32, 2.35, 2.42, 6.14, 7.4, 7.5, 10.2, 10.5, 13.19 al 13.21: El Comité Técnico no logra establecer el cumplimiento de los ítems anteriormente descritos, dado que no se adjuntó ni fue posible identificar, dentro de la información pública en las páginas oficiales del fabricante ofertado, documentación técnica que los respalde, tales como hojas de datos (datasheets), fichas técnicas, descripciones funcionales u otra información oficial relacionada con las capacidades requeridas.

En consecuencia, se solicita al oferente suministrar documentación técnica oficial que permita la verificación objetiva de dichas funcionalidades. Asimismo, deberá indicarse de manera expresa **la fuente y la ubicación exacta dentro de la documentación aportada** (por ejemplo: nombre del documento, sección, capítulo, página, tabla o referencia específica) en la que se evidencie el cumplimiento de cada requisito.

Adicionalmente, en aquellos casos en los que la denominación de la funcionalidad o módulo no corresponda de forma directa con el atributo solicitado, el oferente deberá justificar técnica y detalladamente con qué característica de la solución se satisface la especificación requerida.

Ítem 16.1: No se adjuntó acta de grado del título profesional para el señor EDWIN DANILO VELASCO CALDAS, toda vez, que el documento aportado con el nombre "ACTA DE GRADO INGENIERIA DE TELECOMUNICACIONES.jpeg", no se puede tener en cuenta al ser una certificación.

De la misma manera no anexo certificaciones de experiencia expedidas por el **oferente o fabricante**, es de anotar que no se tienen en cuenta los documentos anexados "Certificación Experiencia Edwin.pdf" y "Certificacion TI360 Edwin Velasco.pdf", por cuanto las expiden empresa externas, sin considerar lo solicitado en el ítem.

Ítem 18.1: No se puede evaluar la experiencia por cuanto no se aportó Registro Único de Proponentes actualizado.

En razón de lo anterior, las empresas podrán subsanar en los términos y tiempos establecidos para el presente proceso, la documentación citada en las especificaciones técnicas.

Atentamente,

Patrullero **DARWIN ALEXIS MONGUI RISCANEVO**
Evaluador técnico proceso PN DIPOL SA 020-2026

Intendente Jefe **WILLIAM LEONARDO APACHE AYALA**
Evaluador técnico proceso PN DIPOL SA 020-2026

Intendente Jefe **WILLIAM VICTORIANO VARGAS VARGAS**
Evaluador técnico proceso PN DIPOL SA 020-2026

Elaboró: PT. DARWIN MONGUI RISCANEVO
DIPOL-CPD

Revisó: IJ. WILLIAM LEONARDO APACHE AYALA
DIPOL-GUTIC

Revisó: IJ. WILLIAM VARGAS VARGAS
DIPOL-CPD

Fecha de elaboración: 23-04-2026
Ubicación: Z:\2026\7.1.4.10.1.3.3 GUTIC\GENERAL\3.COMUNICACIONES OFICIALES

Avenida Boyacá 142A – 55
Teléfono: 5185691
dipol.gutic@dipol.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE INTELIGENCIA POLICIAL
GRUPO PRODUCCIÓN Y ANÁLISIS DE INTELIGENCIA

GS-2026- 016369 **/ARPIN – GRAIN 20.1**

Bogotá D.C., 23 ABR 2026

Señora capitán
ALDEMAR ANDRÉS OSPINA MORALES
Gerente del Proceso PN DIPOL SA 020-2026
Avenida Boyacá 142A-55
Bogotá D.C.

Asunto: evaluación comité jurídico proceso PN DIPOL SA 020-2026

Respetuosamente nos permitimos enviar a mi capitán, la evaluación del comité jurídico realizada en el marco del proceso PN DIPOL SA 020-2026, cuyo objeto es ***"ADQUISICIÓN LICIENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL"***, por valor de doscientos setenta y ocho millones de pesos colombianos ($278.000.000), así:

ÍTEM	ASPECTOS A EVALUAR	OFERENTE	OFERENTE
	Documentos de Orden Jurídico 1.2	**REALTIME CONSULTING & SERVICES S.A.S**	**HIGH TECH SERVICES CORP (HTS CORP)**
1.2.1	Carta de presentación de la oferta formulario No 1.	CUMPLE	CUMPLE
1.2.2	Fotocopia de cédula del representante legal	CUMPLE	CUMPLE
1.2.3	Certificado de Contraloría	CUMPLE	CUMPLE
	Certificado de Procuraduría	CUMPLE	CUMPLE
	Antecedentes Judiciales de Policía Nacional	CUMPLE	CUMPLE
	Inhabilidades Ley 1918 de 2018	CUMPLE	CUMPLE
	Sistema Registro Nacional de Medidas Correctivas	CUMPLE	CUMPLE
1.2.4	Certificado de Registro Único Tributario	CUMPLE	CUMPLE
1.2.5	Certificación expedida por revisor fiscal o declaración juramentada en caso de personal natural o del representante legal del proponente, señalando para el primero el número de la tarjeta profesional y anexando fotocopia de la misma. Si es persona natural, declaración juramentada, en la cual certifique el pago de seguridad social (salud, pensión y riesgos profesionales); y si tiene empleados a su cargo certificar el pago de los aportes parafiscales de sus empleados, indicando que se encuentra al día con dichos pagos (caja de compensación familiar, SENA e instituto colombiano de bienestar familiar). desarrollo del presente numeral se entiende suministrada bajo gravedad de juramento, respecto su	CUMPLE	CUMPLE

	fidelidad y veracidad.		
1.2.6	Compromiso anticorrupción formulario No. 3	CUMPLE	CUMPLE
1.2.7	Compromiso de confidencialidad formulario No. 4	CUMPLE	CUMPLE
1.2.8	Formulario No. 5 SGSST	CUMPLE	CUMPLE
1.2.9	Garantía de seriedad de la oferta por el 10% y cubrir a partir de la fecha de presentación de la oferta y cuatro (4) meses más, expedida a favor de la dirección de inteligencia policial NIT 830.000.097-5 – AV. Boyacá 142a-55 – teléfono 5189223.	CUMPLE	CUMPLE
1.2.10	Certificado de Existencia y Representación Legal vigente, renovada la matricula mercantil para el año 2026. De igual forma, allegar el registro único de proponentes, tener en cuenta que de acuerdo con lo señalado en el artículo 2.2.1.1.1.5.1. del Decreto 1082 de 2015, la renovación de este registro debe realizarse entre el 1.º de enero y a más tardar el quinto (5) día hábil del mes de abril de cada año. De lo contrario, cesarán los efectos, no podrán renovar certificado y deberán realizar una nueva inscripción.	**NO CUMPLE**	**NO CUMPLE**
1.2.11	Verificar que la persona natural o el representante legal de la persona jurídica, no este reportado ante el REDAM Certificación expedida por MINTIC	CUMPLE	CUMPLE
1.2.13	Formato no. 2 inhabilidades e incompatibilidades	**NO CUMPLE**	CUMPLE

Observaciones REALTIME CONSULTING & SERVICES S.A.S

1. **REALTIME CONSULTING & SERVICES S.A.S.:** **NO CUMPLE** con el requisito jurídico habilitante **1.2.10.**, teniendo en cuenta que allegó soporte documental parcial, ya que al verificar no aportó el *"**CERTIFICADO DE INSCRIPCIÓN Y CLASIFICACIÓN REGISTRO ÚNICO DE PROPONENTES**"*.

2. **REALTIME CONSULTING & SERVICES S.A.S** **NO CUMPLE** con el requisito jurídico habilitante **1.2.13.** formulario No. 2, inhabilidades e incompatibilidades, toda vez que no diligenció el documento conforme a lo estipulado por esta entidad.

Observaciones HIGH TECH SERVICES CORP (HTS CORP):

1. **HIGH TECH SERVICES CORP (HTS CORP)**: **NO CUMPLE** con el requisito jurídico habilitante **1.2.10**. con respecto a *"**ALLEGAR EL REGISTRO ÚNICO DE PROPONENTES, TENER EN CUENTA QUE DE ACUERDO CON LO SEÑALADO EN EL ARTÍCULO 2.2.1.1.1.5.1. DEL DECRETO 1082 DE 2015, LA RENOVACIÓN DE ESTE REGISTRO DEBE REALIZARSE ENTRE EL 1º DE ENERO Y A MÁS TARDAR EL QUINTO (5) DÍA HÁBIL DEL MES DE ABRIL DE CADA AÑO**"*, toda vez que el documento presentado por el oferente no fue renovado.

Finalmente, este comité evaluador considera pertinente que le sea **REQUERIDO A LOS OFERENTES LA SUBSANACIÓN DE LOS REQUISITOS JURÍDICOS HABILITANTES**, dentro de los términos de ley establecidos en el pliego de condiciones.

Atentamente,

Intendente **NURY ESNEDY ORTIZ GÓMEZ**
Integrante Comité Jurídico Proceso PN DIPOL SA 020-2026

Subintendente **YERCICA VARGAS MONCADA**
Integrante Comité Jurídico Proceso PN DIPOL SA 020-2026

Patrullero **BLADIMIR SEPULVEDA BORDA**
Integrante Comité Jurídico Proceso PN DIPOL SA 020-2026

Elaboró: Subintendente **YERCICA VARGAS MONCADA**
Responsable Producción de Inteligencia
Área Producción Inteligencia

Revisó: Patrullero **BLADIMIR SEPULVEDA BORDA**
Recolector de Datos
Área Contrainteligencia

Revisó: Intendente **NURY ESNEDY ORTIZ GÓMEZ**
Sustanciador (a)
Grupo Asuntos Jurídicos DIPOL

Fecha de elaboración: 23-04-2025
Ubicación: Z:\2026\GRAIN\JEFAT\DOCUMENTOS DE APOYO 2026\7. Carpetas personales 2026\3. SI. Yercica Vargas Moncada 2026\6. Contratos 2026\PN DIPOL DA 020-2026

Avenida Boyacá 142ª-55
Teléfonos: 5159740
dipol.arpin-gin@dipol.gov.co
www.policia.gov.co

INFORMACIÓN PÚBLICA

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE INTELIGENCIA POLICIAL
GRUPO FINANCIERO Y PRESUPUESTO

GS-2026- 0 1 6 1 4 7 **/ARLOF – GUFIP 20.1**

Bogotá D.C. 22 de abril de 2026

Señor capitán
ALDEMAR ANDRÉS OSPINA MORALES
Gerente invitación PN DIPOL SA 020-2026
Dirección de Inteligencia Policial
Avenida Boyacá 142A - 55
Bogotá D.C.

Asunto: evaluación económica proceso PN DIPOL SA 020-2026.

Respetuosamente me permito remitir a mi capitán, el resultado de la evaluación económica del proceso **PN DIPOL SA 020-2026** que tiene por objeto la **"ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL"**, realizada por los integrantes del comité económico, así:

DOCUMENTOS DE VERIFICACIÓN DE CARÁCTER ECONÓMICO

PROPONENTE	DOCUMENTOS		
	CERTIFICACIÓN BANCARIA	FORMULARIO No. 2	OBSERVACIONES
REALTIME CONSULTING Y SERVICES SAS	CUMPLE	CUMPLE	-
HIGH TECH SERVICES CORP (HTS CORP) S.A.S	CUMPLE	CUMPLE	-

INDICADORES FINANCIEROS

PROPONENTE	REFERENCIA DE INDICADORES				
	ÍNDICE DE LIQUIDEZ *(Menor a 1,57 es excluyente)*	ÍNDICE ENDEUDAMIENTO *(Mayor a 0,71 excluyente)*	*ÍNDICE RAZÓN DE COBERTURA DE INTERÉS (Menor a 1 excluyente)*	ÍNDICE RENTABILIDAD DEL ACTIVO *(Menor a 0,05 excluyente)*	ÍNDICE RENTABILIDAD PATRIMONIO *(Menor a 0,09 excluyente)*
REALTIME CONSULTING Y SERVICES SAS	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE
HIGH TECH SERVICES CORP (HTS CORP) S.A.S	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE

OBSERVACIONES:

PROPONENTES	OBSERVACIONES
REALTIME CONSULTING Y SERVICES SAS	En atención a que el proponente NO anexó el RUP, el cual se encuentra establecido dentro de los pliegos definitivos en el ítem 1.3 **Requisitos Económicos Habilitantes desde el numeral 1.3.2 hasta el 1.3.5** *"El oferente deberá anexar el registro único de proponentes - RUP, tener en cuenta que de acuerdo con lo señalado en el artículo 2.2.1.1.1.5.1. del Decreto 1082 de 2015, la renovación de este registro debe realizarse entre el 1° de enero y a más tardar el quinto (5) día hábil del mes de abril de cada año. De lo contrario, cesarán los efectos, no podrán solicitar certificado y deberán realizar una nueva inscripción".*

	Por lo anterior, se requiere que el oferente remita el RUP, con el fin de verificar el cumplimiento de los indicadores financieros dentro de los plazos establecidos.
HIGH TECH SERVICES CORP (HTS CORP) S.A.S	Para determinar el cumplimiento de los indicadores financieros se revisó el Registro Único de Proponentes – RUP allegado por parte del oferente, evidenciándose que el mismo presenta como fecha de renovación el 09/04/2025; motivo por el cual no se puede hacer la valoración de los indicadores en mención de la vigencia 2025. Frente a lo anterior, se observa que la capacidad financiera y organizacional del proponente, presentan un reporte a corte 31/12/2024. CERTIFICA: IDENTIFICACION QUE: HIGH TECH SERVICES CORP (HTS CORP) S.A.S. NIT: 901121717 1 NUMERO DEL PROPONENTE EN LA CAMARA DE COMERCIO: 00069351 CERTIFICA: INSCRIPCION Y RENOVACION FECHA DE INSCRIPCION EN EL REGISTRO DE LOS PROPONENTES: 2020/07/29 FECHA DE ULTIMA RENOVACION EN EL REGISTRO DE LOS PROPONENTES: 2025/04/09

En consecuencia, nos permitimos indicar a mi capitán, que los oferentes podrán subsanar los documentos anteriormente requeridos en los términos del cronograma del presente proceso, a través de la plataforma SECOP II.

Atentamente,

Subintendente **YURLEY SABINA PUENTES ARCHILA**
Integrante Comité Económico Evaluador PN DIPOL SA 020-2026

Intendente jefe **ALBERTO ALEXANDER PULIDO QUEVEDO**
Integrante Comité Económico Evaluador PN DIPOL SA 020-2026

Subcomisario **JOSÉ FERNANDO OLIVAR SALDAÑA**
Integrante Comité Económico Evaluador PN DIPOL SA 020-2026

Elaboró: Subintendente **YURLEY SABINA PUENTES ARCHILA**
Auxiliar de Tesorería

Revisó: Intendente jefe **ALBERTO ALEXANDER PULIDO QUEVEDO**
Investigador en Ciencia, Tecnología e Innovación

Revisó: Subcomisario **JOSÉ FERNANDO OLIVAR SALDAÑA**
Responsable de Bienes Inmuebles

Fecha de elaboración: 22/06/2026
Ubicación: Y:\2026\2.2.2.8.6 ARLOF\DOCUMENTOS DE APOYO\10. FUNCIONARIOS JEFATURA\SI. SABINA\COMITES ECONOMICOS

Avenida Boyacá 142A - 55
Teléfono: 5159629
dipol.arlof-fin@dipol.gov.co
www.policia.gov.co

INFORMACION PÚBLICA