MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

DIRECCIÓN DE INTELIGENCIA POLICIAL

CONTRATO DE COMPRAVENTA PN DIPOL SA No. 04-2-10024-2026 CELEBRADO ENTRE LA DIRECCIÓN DE INTELIGENCIA POLICIAL Y HIGH TECH SERVICES CORP (HTS CORP) S.A.S., 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.

Entre los suscritos, de una parte la **POLICÍA NACIONAL – DIRECCIÓN DE INTELIGENCIA POLICIAL**, quien actúa a través de su representante legal o su delegado, quien en adelante se denominará la **DIRECCIÓN DE INTELIGENCIA POLICIAL**, y por la otra, el **CONTRATISTA**, debidamente identificados como aparece en el anexo No.1 "DATOS DEL CONTRATO", hemos convenido celebrar el presente contrato, previos los siguientes considerandos: **a)** Que se elaboraron los estudios previos de conformidad con lo señalado en el Decreto 1082 de 2015 **b)** Que al momento de la apertura del proceso de selección, se contó con la respectiva apropiación presupuestal que respalda el presente compromiso. **c)** La ley 1150 de 2007, "por medio de la cual se introduce medidas para la eficiencia y transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos"; establece en el artículo 2 las Modalidades de Selección, en el numeral 2 figura la Selección Abreviada, la cual procederá en los siguientes casos: (...) literal a, "La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que correspondan a aquellos que poseen las mismas especificaciones técnicas con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos", en concordancia con el Decreto 1082 del 2015. **d)** Que la **DIRECCIÓN DE INTELIGENCIA POLICIAL** designará un supervisor para el presente contrato, el cual mantendrá comunicación con el **CONTRATISTA**, durante el desarrollo del contrato y ejercerá las funciones prescritas en la Resolución 00090 del 16 de enero de 2018 de la Policía Nacional. **e)** Que habiéndose dado cumplimiento a todos los trámites y requisitos que exige la contratación administrativa para este tipo de contrato (Ley 80 de 1993, Ley 1150 de 2007 y el Decreto 1082 de 2015), es procedente la celebración del mismo, el cual se regirá por las siguientes clausulas: ***PRIMERA. OBJETO*****:** El objeto del presente contrato es el que se indica el Anexo No.1 "DATOS DEL CONTRATO". ***SEGUNDA. FINALIDADES DEL CONTRATO*****:** El presente contrato está orientado a lograr la efectiva y eficiente prestación del servicio propio de la Policía Nacional, en consecuencia, el **CONTRATISTA** se compromete para con la **DIRECCIÓN DE INTELIGENCIA POLICIAL** a prestar el servicio requerido para suplir las necesidades definidas en los estudios previos. En tal sentido, queda claro que todas las obligaciones a cargo del **CONTRATISTA**, derivadas del presente contrato, así como de la naturaleza de su objeto y las finalidades por él previstas, son obligaciones de resultado. Estas finalidades deberán tenerse en cuenta para la adecuada comprensión e interpretación del presente contrato, especialmente en lo que concierne a sus reglas y condiciones, así como para determinar el alcance de los derechos y obligaciones que el mismo atribuye a las partes. ***TERCERA. VALOR*****:** Para efectos legales, fiscales y presupuestales, el valor del contrato asciende a la suma descrita en el anexo No.1 "DATOS DEL CONTRATO". **PARÁGRAFO:** Todos los precios aquí contemplados se entienden firmes y fijos y por lo tanto no están sujetos a ninguna clase de reajuste. Igualmente, dentro de este precio están incluidos los costos proyectados al plazo de ejecución del presente contrato y la utilidad razonable que el **CONTRATISTA** pretende obtener, en consecuencia, no se aceptarán solicitudes de reajustes, fundamentados en estas circunstancias. ***CUARTA. FORMA DE PAGO*****: LA DIRECCIÓN DE INTELIGENCIA POLICIAL** pagará al **CONTRATISTA** el valor de este contrato de conformidad

con lo dispuesto en el anexo No.1 "DATOS DEL CONTRATO". **PARAGRAFO PRIMERO:** el pago se realizará en moneda legal colombiana, en forma total, dentro de los sesenta (60) días calendario siguientes a la radicación de la factura, junto con el recibido a satisfacción de los elementos adquiridos, suscrito por el supervisor del contrato, junto con los documentos requeridos por el Área Logística y Financiera de la Dirección de Inteligencia Policial, de acuerdo al derecho a turno y la programación del plan anual de caja (PAC). **NOTA:** Para la facturación deberá tener en cuenta la circular 000003 del 16/04/2021 de la Dirección de Impuestos y Aduanas Nacionales y la Resolución 000202 del 31 de marzo de 2025 "Por medio de la cual se modifica parcialmente la Resolución 000165 del 1 de noviembre de 2023", donde se dan a conocer parámetros a los contratistas, proveedores, y supervisores en la recepción de facturas electrónicas a través del Sistema Integrado de Información Financiera SIIF. **PARÁGRAFO SEGUNDO - CUENTA PARA PAGOS:** Los pagos previstos en esta cláusula se acreditarán a la cuenta que se indica en el anexo No.1 "DATOS DEL CONTRATO", a favor del **CONTRATISTA**, o en otro banco o cuenta que éste designe con anterioridad al vencimiento del pago, con sujeción a lo previsto en las disposiciones cambiarias, por medio de aviso escrito con no menos treinta (30) días de anticipación, acompañado de certificación bancaria a nombre de la firma Contratista. Todos los pagos efectuados tendrán los descuentos de ley. ***QUINTA. APROPIACIÓN PRESUPUESTAL*:** El presente contrato está amparado por la apropiación presupuestal que se indica en el anexo No.1 "DATOS DEL CONTRATO". ***SEXTA. PLAZO DE EJECUCIÓN*:** El plazo de ejecución del contrato es el señalado en el anexo No.1 "DATOS DEL CONTRATO". ***SÉPTIMA. VIGENCIA*:** la vigencia del presente contrato será de cuatro (4) meses adicionales al plazo de ejecución establecido en el anexo No.1 "DATOS DEL CONTRATO". ***OCTAVA. LUGAR DE ENTREGA*:** El sitio en el cual aparece en el anexo No.1 "DATOS DEL CONTRATO". ***NOVENA. DERECHOS DEL CONTRATISTA*:** En general, son derechos del **CONTRATISTA**: **1.)** Recibir el pago que en su favor establece el presente contrato. **2.)** Tener acceso a los elementos físicos necesarios para desarrollar el objeto del contrato, en caso que los mismos sean necesarios, y cumplir con sus obligaciones. **3.)** Obtener la colaboración necesaria de la Policía para el adecuado desarrollo del contrato. ***DÉCIMA. OBLIGACIONES DEL CONTRATISTA*:** En general, son obligaciones del **CONTRATISTA:** 1. Cumplir con el objeto contractual. 2. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y trabas. 3. Responder en los plazos que la **DIRECCIÓN DE INTELIGENCIA POLICIAL** establezca en cada caso, los requerimientos de aclaración o de información que le formule. 4. Cumplir cabalmente con sus obligaciones, frente al Sistema de Seguridad Social Integral y parafiscales (Cajas de Compensación Familiar, Sena e ICBF), por cuanto el cumplimiento de esta obligación es requisito indispensable para la realización de cualquier pago. 5. Constituir en debida forma y aportar al Grupo Contractual y Seguimiento de la **DIRECCIÓN DE INTELIGENCIA POLICIAL** o quien haga sus veces, dentro de los tres (3) días hábiles siguientes a la suscripción del contrato, la Garantía Única. 6. Guardar la confidencialidad de toda la información que le sea entregada y que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o manipular y responderá civil, penal y disciplinariamente por los perjuicios de su divulgación y/o utilización indebida que por sí o por un tercero se cause a la administración o a terceros. 7. No acceder a peticiones o amenazas, de quienes actuando por fuera de la ley pretendan obligarlo a hacer u omitir algún acto o hecho, el **CONTRATISTA** deberá informar de tal evento a la **DIRECCIÓN DE INTELIGENCIA POLICIAL** y a las autoridades competentes para que se adopte las medidas necesarias. 8. Mantener activa la cuenta corriente o de ahorros reportada para los pagos con el fin de evitar traumatismos en el proceso de ejecución del contrato. 9. Restituir a **DIRECCIÓN DE INTELIGENCIA POLICIAL** los elementos que haya colocado a su disposición para el desarrollo del objeto contractual, cuando se lo requiera o al finalizar el contrato, en caso de que se hayan suministrado. 10. Incluir todas aquellas obligaciones que el contratista debe cumplir con el fin de alinear la actividad contractual a las buenas prácticas en materia ambiental. Tener además en cuenta lo establecido en la resolución 03049 del 2014, "Por medio del cual se adopta el Manual de Contratación de la Policía Nacional", actualizada, modificada y complementada por las Resoluciones Nos. 00090

del 2018 apéndice 1 y apéndice 2 del 2020. 11. Así mismo incluir las obligaciones en materia de Seguridad y Salud en el Trabajo y los lineamientos del gobierno nacional en el tema del COVID. 12. Para la facturación deberá tener en cuenta la circular 000003 del 16/04/2021 de la Dirección de Impuestos y Aduanas Nacionales y la Resolución 000202 del 31 de marzo de 2025 "Por medio de la cual se modifica parcialmente la Resolución 000165 del 1 de noviembre de 2023", donde se dan a conocer parámetros a los contratistas, proveedores, y supervisores en la recepción de facturas electrónicas a través del Sistema Integrado de Información Financiera SIIF. 13. Las demás obligaciones del CONTRATISTA contenidas en el artículo 5º de la Ley 80 de 1993, así mismo, será civil y penalmente responsable por sus acciones u omisiones en la actuación contractual. ***DÉCIMA PRIMERA. DERECHOS DE LA POLICÍA NACIONAL:*** Supervisar el desarrollo y ejecución del presente contrato, y acceder a los documentos e información que soportan la labor del CONTRATISTA. ***DÉCIMA SEGUNDA. OBLIGACIONES DE LA POLICÍA NACIONAL:*** 1. Poner a disposición del CONTRATISTA los bienes y lugares que se requieran para la ejecución y entrega del objeto contratado. 2. Una vez se surta el proceso de contratación estatal, asignar un supervisor, a través de quien la **DIRECCIÓN DE INTELIGENCIA POLICIAL** mantendrá la interlocución permanente y directa con el **CONTRATISTA**. 3. Ejercer el control sobre el cumplimiento del contrato a través del supervisor designado para el efecto, exigiéndole la ejecución idónea y oportuna del objeto a contratar. 4. Recibir a satisfacción los bienes y/o servicios que sean entregados por el **CONTRATISTA,** cuando estos cumplan con las condiciones establecidas y en especial las especificaciones u obligaciones técnicas contenidas en el anexo técnico. 5. Adelantar las gestiones necesarias para el reconocimiento y cobro de las sanciones pecuniarias y garantías a que hubiere lugar, para lo cual el supervisor dará aviso oportuno a la **DIRECCIÓN DE INTELIGENCIA POLICIAL**, sobre la ocurrencia de hechos constitutivos de mora o incumplimiento. 6. Pagar al **CONTRATISTA** en la forma pactada y con sujeción a las disponibilidades presupuestales y de PAC previstas para el efecto. 7. Tramitar diligentemente las apropiaciones presupuestales que requiera para solventar las prestaciones patrimoniales que hayan surgido a su cargo como consecuencia de la suscripción del contrato. 8. Solicitar y recibir información técnica respecto del bien o servicio y demás del **CONTRATISTA** en desarrollo del objeto del contractual. 9. Incluir aquellas obligaciones propias de cada proceso que coadyuven al cumplimiento de las obligaciones contractuales. 10. Rechazar los bienes y/o servicios cuando no cumplan con los requerimientos técnicos exigidos. ***DÉCIMA TERCERA. RESERVA DEL PRESENTE CONTRATO:*** El **CONTRATISTA** se obliga para con la **DIRECCIÓN DE INTELIGENCIA POLICIAL** a no suministrar ninguna clase de información o detalle a terceros y a mantener como documentación reservada, todos los aspectos que conozca en el cumplimiento del presente contrato, así como los asuntos técnicos e instalaciones de la Policía Nacional, conocidos o que llegaren a ser conocidos por el contratista, durante el desarrollo con posterioridad a la ejecución del contrato. ***DÉCIMA CUARTA. MECANISMO DE COBERTURA DEL RIESGO A CARGO DEL CONTRATISTA:*** Dentro de los tres (3) días hábiles siguientes a la suscripción y registro del contrato y la entrega de la copia firmada del mismo al **CONTRATISTA,** éste deberá constituir y presentar a favor de la **DIRECCIÓN DE INTELIGENCIA POLICIAL**, uno cualquiera de los mecanismos de cobertura de riesgo establecidos en el Decreto 1082 del 2015, que cubra los siguientes riesgos: a) **DE CUMPLIMIENTO DEL CONTRATO:** por el veinte por ciento (20%) del valor total del contrato, vigente por un término igual a la vigencia del contrato y sesenta (60) días calendario más. b) **CALIDAD DEL SERVICIO:** por el cincuenta por ciento (50%) del valor del contrato, vigente por un término igual a la vigencia del contrato y treinta y tres (33) meses más. c) **NO PAGO DE SALARIOS, PRESTACIONES E INDEMNIZACIONES LABORALES:** por el cinco por ciento (5%) del valor del contrato, vigente por un término igual a la vigencia del contrato y tres (03) años más. **PARÁGRAFO PRIMERO: <u>En la póliza de garantía única deberá constar expresamente que se ampara el cumplimiento del contrato, el pago de las multas y de la penal pecuniaria convenidas y que la entidad aseguradora renuncia al beneficio de excusión.</u> Así mismo, se indicará que en el evento en que por incumplimiento del contratista garantizado el asegurador resolviera continuar, como cesionario, con la**

ejecución del contrato y la entidad estatal contratante estuviere de acuerdo con ello, el contratista garantizado aceptará desde el momento de contratación de la póliza la cesión del contrato a favor del asegurador. En todo caso, dependiendo del tipo de mecanismo de cobertura elegido, deberá cumplir con los requisitos establecidos en el Decreto 1082 de 2015. ***DÉCIMA QUINTA. INDEMNIDAD***: El **CONTRATISTA** se obliga a mantener indemne a la POLICÍA NACIONAL de cualquier reclamación proveniente de terceros que tenga como causa sus actuaciones. ***DÉCIMA SEXTA. SANCIONES***: **a) MULTAS**.- En caso de mora o incumplimiento parcial de alguna de las obligaciones derivadas del presente contrato por causas imputables al **CONTRATISTA** - salvo circunstancias de fuerza mayor o caso fortuito conforme a las definiciones del artículo 1º de la Ley 95 de 1.890 –las partes acuerdan que la **DIRECCIÓN DE INTELIGENCIA POLICIAL**, mediante acto administrativo, afectará al **CONTRATISTA** con multas, cuyo valor se liquidará con base en el cero punto cinco por ciento (0,5%) del valor dejado de entregar, por cada día de retardo y hasta por quince (15) días calendario. Esta sanción se impondrá conforme a la ley y se reportará a la Cámara de Comercio competente de conformidad con lo previsto en el artículo 6º de la Ley 1150 de 2007. **b). MULTA POR LA MORA EN LA CONSTITUCIÓN DE LOS REQUISITOS DE EJECUCIÓN Y LEGALIZACIÓN:** Cuando el contratista no constituya dentro del término y en la forma prevista en el contrato, o en alguno de sus modificatorios, la póliza de garantía única, en caso de existir, y/o alguno de los requisitos de legalización, la **POLICÍA** podrá mediante acto administrativo afectar al **CONTRATISTA** con multa, cuyo valor se liquidará con base en un cero punto dos por ciento (0,2%) del valor del contrato, por cada día de retardo y hasta por diez (10) días. **c) PENAL PECUNIARIA**. En caso de declaratoria de caducidad o de incumplimiento total de las obligaciones derivadas del presente contrato, **EL CONTRATISTA** pagará a la **DIRECCIÓN DE INTELIGENCIA POLICIAL**, a título de pena pecuniaria, una suma equivalente al veinte por ciento (20%) del valor del contrato cuando se trate de incumplimiento total del contrato y proporcional al incumplimiento parcial del contrato que no supere el porcentaje señalado. Para efectos de calcular el monto del incumplimiento parcial relativo a la obligación de plazo de ejecución, se empleará la misma fórmula de estimación de valor contemplada en el literal a) del presente artículo. La imposición de esta pena pecuniaria se considerará como pago parcial y definitivo de los perjuicios que cause a la **DIRECCIÓN DE INTELIGENCIA POLICIAL**. No obstante, la **DIRECCIÓN DE INTELIGENCIA POLICIAL** se reserva el derecho de cobrar perjuicios adicionales por encima del monto de lo aquí pactado, siempre que los mismos se acrediten. El pago de la cláusula penal pecuniaria estará amparado mediante póliza de seguros en las condiciones establecidas en el presente contrato. **PARÁGRAFO. APLICACIÓN DEL VALOR DE LAS SANCIONES PECUNIARIAS:** Una vez notificada la resolución por medio de la cual se imponen alguna de las sanciones antes descritas, el **CONTRATISTA** dispondrá de quince (15) días calendario para proceder de manera voluntaria para su pago. Las multas no serán reintegrables aún en el supuesto que el **CONTRATISTA** dé posterior ejecución a la obligación incumplida. En caso de no pago voluntario y una vez en firme la resolución que imponga multas, podrá tomarse del saldo a favor del **CONTRATISTA** si lo hubiere, o acudir a la jurisdicción coactiva. ***DÉCIMA SÉPTIMA CADUCIDAD ADMINISTRATIVA***: Si se presenta algún hecho constitutivo de incumplimiento de las obligaciones a cargo del **CONTRATISTA**, que afecte de manera grave y directa la ejecución del contrato y evidencie que puede conducir a su paralización, la **DIRECCIÓN DE INTELIGENCIA POLICIAL** por medio de acto administrativo debidamente motivado podrá decretar la caducidad y ordenar la liquidación en el estado en que se encuentre, todo de conformidad con lo previsto en el artículo 18 de la Ley 80 de 1.993. Ejecutoriada la resolución de caducidad, el contrato quedará definitivamente terminado y el **CONTRATISTA** no tendrá derecho a reclamar indemnización alguna. La **DIRECCIÓN DE INTELIGENCIA POLICIAL**, hará efectivo el valor de la pena pecuniaria, y procederá a su liquidación. Para efectos de esta liquidación, el **CONTRATISTA** devolverá a la **DIRECCIÓN DE INTELIGENCIA POLICIAL** los dineros que hubiere recibido por concepto del presente contrato, previa deducción del valor de los elementos entregados por aquel y recibidos a satisfacción por la **DIRECCIÓN DE INTELIGENCIA POLICIAL** de conformidad con lo establecido en la cláusula

primera del presente contrato. En el acta de liquidación se determinarán las obligaciones a cargo de las partes, teniendo en cuenta el valor de las sanciones por aplicar o las indemnizaciones a cargo la **DIRECCIÓN DE INTELIGENCIA POLICIAL**, si a esto hubiere lugar, y la fecha de pago. ***DÉCIMA OCTAVA. OTRAS FACULTADES EXCEPCIONALES***: En caso de presentarse cualquiera de las circunstancias establecidas en los artículos 15, 16 y 17 de la Ley 80/93, debidamente establecidas y documentadas, la **DIRECCIÓN DE INTELIGENCIA POLICIAL** podrá hacer uso de las facultades excepcionales allí previstas, en caso que las mismas resulten aplicables. ***DÉCIMA NOVENA. MONEDA DEL CONTRATO:*** La moneda del presente contrato es la indicada en el anexo No.1 DATOS DEL CONTRATO. ***VIGÉSIMA. CESIONES Y SUBCONTRATOS***: **El CONTRATISTA** no podrá ceder en todo o en parte el presente contrato a persona alguna natural o jurídica, nacional o extranjera, sin previa autorización escrita de la **DIRECCIÓN DE INTELIGENCIA POLICIAL**, pudiendo esta reservarse las razones que tenga para negar dicha autorización. La celebración de subcontratos no relevará al **CONTRATISTA** de las responsabilidades que asume en virtud del presente contrato. La **DIRECCIÓN DE INTELIGENCIA POLICIAL** no adquirirá relación alguna con los Subcontratistas. ***VIGÉSIMA PRIMERA. INHABILIDADES E INCOMPATIBILIDADES***: **El CONTRATISTA** declara bajo la gravedad del juramento, la cual se entenderá cumplida con la suscripción del presente Contrato, que no se halla incurso en ninguna de las causales de inhabilidad o incompatibilidad señaladas en la ley. ***VIGÉSIMA SEGUNDA. SUSPENSIÓN TEMPORAL:*** Las partes podrán suspender temporalmente el plazo de ejecución del contrato, cuando se presenten causas que impidan la ejecución temporal o transitoria, por ocurrencia de un imprevisto o hecho inevitable, una vez establecida en debida forma la causal se suscribirá un acta entre las partes, donde conste el evento, su causa, el término de la suspensión y aquellas previsiones que se consideren necesario consignar. El tiempo de suspensión no se computará para los efectos del plazo extintivo del presente contrato. Para el reinicio de la ejecución y, superada la situación que originó la suspensión del plazo de ejecución, se suscribirá la correspondiente acta de reinicio. ***VIGÉSIMA TERCERA. SOLUCIÓN DE CONFLICTOS***: Si con ocasión del desarrollo y ejecución del contrato, sugieren diferencias o discrepancias entre las partes, estas se comprometen a utilizar los mecanismos de solución directa previstos en el artículo 68 de la Ley 80 de 1993. ***VIGÉSIMA CUARTA. PERFECCIONAMIENTO, LEGALIZACIÓN Y EJECUCIÓN***: Para el perfeccionamiento del presente contrato se requiere de las firmas de las partes y del correspondiente registro presupuestal. Para su **legalización** y **ejecución** se requiere de la aprobación por parte de la **DIRECCIÓN DE INTELIGENCIA POLICIAL** del mecanismo de cobertura de riesgos, constituido por parte del **CONTRATISTA**. **PARÁGRAFO. -** Dentro de los tres (3) días hábiles siguientes a la firma del contrato y entrega de una copia del mismo al **CONTRATISTA**, éste se obliga a presentar los recibos de consignación correspondientes y el mecanismo de cobertura de riesgos en la oficina del Grupo de Contratos del Área Logística y Financiera de la **DIRECCIÓN DE INTELIGENCIA POLICIAL**. Las sanciones que ocasionen su no pago oportuno y la no entrega de los respectivos documentos a la **DIRECCIÓN DE INTELIGENCIA POLICIAL** dentro del término antes fijado, serán a cargo del **CONTRATISTA**. ***VIGÉSIMA QUINTA. DOCUMENTOS***: Entre otros, los documentos que a continuación se relacionan se consideran para todos los efectos parte integrante del presente contrato y en consecuencia producen sus mismos efectos u obligaciones jurídicas y contractuales: **1.)** Invitación a presentar oferta. **2.)** Propuesta del Contratista en aquellas partes aceptadas por la **DIRECCIÓN DE INTELIGENCIA POLICIAL 3).** Anexos del contrato. **4.)** Documentos que suscriban las partes. ***VIGÉSIMA SEXTA. IMPUESTOS***: **El CONTRATISTA** pagará todos los impuestos, tasas, contribuciones y similares que se deriven de la ejecución del contrato, de conformidad con la ley colombiana. ***VIGÉSIMA SÉPTIMA. LIQUIDACIÓN***: El presente contrato se podrá liquidar de conformidad con lo señalado en los artículos 60 de la Ley 80 de 1993 y artículo 11 de la Ley 1150 de 2007. ***VIGÉSIMA OCTAVA. VEEDURÍAS CIUDADANAS***: el presente contrato está sujeto a la vigilancia y control ciudadano, en los términos que señala el artículo 66 de la Ley 80 de 1993. ***VIGÉSIMA NOVENA. RÉGIMEN LEGAL***: Este contrato se regirá por el Estatuto General de Contratación Administrativa vigente y sus decretos

reglamentarios, las leyes de presupuesto, en general las normas civiles y comerciales vigentes, las demás normas concordantes que rijan o lleguen a regir los aspectos del presente contrato y las disposiciones de la Policía Nacional que apliquen. ***TRIGÉSIMA*: DOMICILIO CONTRACTUAL:** Para todos los efectos, las partes acuerdan como domicilio contractual el Distrito Capital de Bogotá, para constancia de lo anterior, se firma en un (1) original en Bogotá, D.C., a los 19 MAY 2026

LA DIRECCIÓN DE INTELIGENCIA POLICIAL

Brigadier general **RICARDO SÁNCHEZ SILVESTRE**
Director de Inteligencia Policial

CONTRATISTA

Laura Marcela Cepeda S.

LAURA MARCELA CEPEDA SANABRIA
Representante Legal: HIGH TECH SERVICES CORP (HTS CORP) S.A.S.

Elaboró IJ. Edison Alexander Gutiérrez González	Vo. Bo. / SI. Deyri Daniela Duarte Duarte	Vo. Bo.___ / MY. Pedro David Montdragón Piñeros
Analista de contratos	Sustanciador	Jefe Grupo de Contratos
Vo. Bo.___ / MY. Alexander Malagón Aguillón	Vo. Bo.___ / TC. Henry Giovanny Sánchez Holguín	Vo. Bo.___ / CR. José Manuel Alvarez Omaña
Jefe Grupo Asuntos Jurídicos	Jefe Área Logística y Financiera	Subdirector de Inteligencia Policial

ANEXO No.1
"DATOS DEL CONTRATO"

CONTRATO	**No. 04-2-10024-2026**
CONTRATANTE	DIRECCIÓN DE INTELIGENCIA POLICIAL
REPRESENTANTE LEGAL Y/O DELEGADO	Brigadier general RICARDO SÁNCHEZ SILVESTRE
CÉDULA DE CIUDADANÍA No.	17.416.370 de Acacías (Meta)
CARGO	Director de Inteligencia Policial
DISPOSICION DE NOMBRAMIENTO	Decreto No. 0259 del 16 de marzo de 2026
RESOLUCIÓN DE DELEGACIÓN	Resolución No. 00502 del 05 de marzo de 2026
CONTRATISTA	**NOMBRE:** HIGH TECH SERVICES CORP (HTS CORP) S.A.S. **NIT:** 901121717-1 **REPRESENTANTE LEGAL:** Laura Marcela Cepeda Sanabria **CÉDULA DE CIUDADANÍA No.** 63.438.592 de Velez **CIUDAD NOTIFICACIÓN:** Bogotá D.C. **DIRECCIÓN:** Calle 19 No. 4-74 Oficina 1801 **TELÉFONO:** 601-5191226 **CELULAR:** 3043423718 **E-MAIL:** gerencia.comercial@htscorp.com.co
CONSIDERANDOS	Que el presente contrato se deriva del PN DIPOL SA 020-2026 **ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL.**
SUPERVISOR DEL CONTRATO	La supervisión del contrato estará a cargo del jefe del Centro de Protección de Datos de la Dirección de Inteligencia Policial o quien haga sus veces, o quien con posterioridad sea designado por parte del Director de Inteligencia Policial, quien verificará la ejecución idónea y el cumplimiento del objeto del contrato de acuerdo con las funciones asignadas para el efecto en la Resolución No. 00090 del 15 de enero del 2018.
CLAUSULA PRIMERA. - OBJETO	El objeto del presente contrato es: **ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL.** ITEM: 1 — RECURSO: 10 — UNIDAD: DIPOL
CLAUSULA TERCERA. - VALOR	Para efectos legales y presupuestales, el valor total del contrato asciende a la suma de **DOSCIENTOS SETENTA Y SIETE MILLONES SETECIENTOS NOVENTA Y NUEVE MIL NOVECIENTOS PESOS ($ 277.799.900) EXENTO IVA*.**

ÍTEM	DESCRIPCIÓN	CANT	VALOR UNITARIO EXENTO DE IVA*	VALOR TOTAL EXENTO DE IVA*
1	ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL	1	$ 277.799.900,00	$ 277.799.900,00
			VALOR TOTAL	$ 277.799.900,00

Nota Aclaratoria: El bien objeto de adquisición se encuentra catalogado como exento, de acuerdo a lo dispuesto en el artículo 188 del decreto 1819 de 2016, que modifica el artículo 477 del Estatuto Tributario. Bienes que se encuentran exentos del impuesto, literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional. Atendiendo su naturaleza y destinación estos bienes se encuentran gravados a la tarifa 0%.

CLAUSULA CUARTA. - FORMA DE PAGO	El pago se realizará en moneda legal colombiana, en forma total, dentro de los sesenta (60) días calendario siguientes a la radicación de la factura, junto con el recibido a satisfacción de los elementos adquiridos, suscrito por el supervisor del contrato, junto con los documentos requeridos por el Área Logística y Financiera de la Dirección de Inteligencia Policial, de acuerdo al derecho a turno y la programación del plan anual de caja (PAC). Si los documentos en referencia no se reciben dentro del plazo establecido o, si recibidos son devueltos por inconsistencias tales como la falta de información o mal diligenciamiento de los mismos, la Policía Nacional – Dirección de Inteligencia Policial, programará el valor a cancelar una vez se hubieren subsanado las observaciones, se haya cumplido con el trámite documental dentro del plazo indicado y de acuerdo al derecho a turno y la disponibilidad del Plan Anual de Caja (PAC). Si los documentos en referencia son devueltos por la DIRECCIÓN DE INTELIGENCIA POLICIAL, por inconsistencias como la falta de información o mal diligenciamiento de los mismos, la DIRECCIÓN DE INTELIGENCIA POLICIAL, se obliga a la asignación nuevamente del turno, siempre y cuando se hubieren subsanado las observaciones y se haya cumplido con el trámite documental dentro del plazo indicado. El contratista deberá presentar con la oferta la Certificación de existencia de cuenta corriente o de ahorros expedida por la entidad bancaria. El recibido a satisfacción, aunque se encuentre suscrito por el supervisor del contrato, no implica el recibo o aprobación definitiva por parte de la DIRECCIÓN DE INTELIGENCIA POLICIAL del bien o servicio suministrado (según corresponda) y por consiguiente, no exime al CONTRATISTA de su responsabilidad en cuanto a la calidad, cantidad y buena calidad del bien o servicio contratado o de cualquier otra obligación contractual o de responsabilidad civil. Si el recibido a satisfacción no ha sido bien elaborado o no se acompaña a esta de los documentos que para cada caso se soliciten en esta contratación, los términos anteriores sólo empezarán a contarse desde la fecha en que quede corregida el acta o desde aquella en que se haya aportado el último de los documentos. Todas las demoras que se presenten por estos conceptos serán de responsabilidad del CONTRATISTA, quien no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza. Lo mismo se predicará en el caso de que el CONTRATISTA no elabore y presente las respectivas actas a la DIRECCIÓN DE INTELIGENCIA POLICIAL. **NOTA:** Para la facturación deberá tener en cuenta la circular 000003 del 16/04/2021 de la Dirección de Impuestos y Aduanas Nacionales y la Resolución 000202 del 31 de marzo de 2025 "Por medio de la cual se modifica parcialmente la Resolución 000165 del 1 de noviembre de 2023", donde se dan a conocer parámetros a los contratistas, proveedores, y supervisores en la recepción de facturas electrónicas a través del Sistema Integrado de Información Financiera SIIF. La ruta donde puede realizar la consulta de pago la ubica en: http://www.minhacienda.gov.co/MinHacienda/haciendapublica/siifnacion/SIIFNacion/consulta%20de%20pagos

	Los pagos se harán a la siguiente cuenta: **NOMBRE BENEFICIARIO:** HIGH TECH SERVICES CORP (HTS CORP) S.A.S. **BANCO**: DAVIVIENDA **TIPO DE CUENTA:** AHORROS **NUMERO DE CUENTA:** 046170485026 **OFICINA:** Bogotá D.C.
CLAUSULA QUINTA. - APROPIACIÓN PRESUPUESTAL	El presente contrato está respaldado por el certificado de disponibilidad presupuestal No. 4226.
CLAUSULA SEXTA. - PLAZO DE EJECUCIÓN	La ejecución del contrato será a partir del día hábil siguiente a la aprobación de la garantía única y hasta el 10 de agosto del 2026.
CLAUSULA OCTAVA: LUGAR DE ENTREGA DE LOS BIENES	El licenciamiento objeto de la contratación deberá ser entregado en la ciudad de Bogotá, Dirección de Inteligencia Policial ubicada en la Avenida Boyacá No. 142 A-55 Bogotá D.C., barrio Colina Campestre.
CLAUSULA DÉCIMA OCTAVA - MONEDA DEL CONTRATO	Pesos colombianos

LA DIRECCIÓN DE INTELIGENCIA POLICIAL

Brigadier general **RICARDO SÁNCHEZ SILVESTRE**
Director de Inteligencia Policial

CONTRATISTA

Laura Marcela Cepeda S.

LAURA MARCELA CEPEDA SANABRIA
Representante Legal: HIGH TECH SERVICES CORP (HTS CORP) S.A.S.

Elaboró: Edison Alexander Gutiérrez González Analista de contratos	Vo. Bo. / SI. Deyri Daniela Duarte Duarte Sustanciador	Vo. Bo. / MY. Pedro David Arbeláez Piñeros Jefe Grupo de Contratos
Vo. Bo. / MY. Alexander Malagón Aguillón Jefe Grupo Asuntos Juridicos	Vo. Bo. / TC. Henry Giovanny Sánchez Holguín Jefe Área Logística y Financiera	Vo. Bo. / CR. José Manuel Alvarez Omaña Subdirector de Inteligencia Policial

ANEXO 2
ESPECIFICACIONES TECNICAS MINIMAS

ÍTEM	DESCRIPCIÓN
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.
1.2	**MARCA:** Trend AI **REFERENCIA:** TREND VISION ONE **FABRICANTE:** 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
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
2.3	La solución deberá tener motores para la detección de malware con la capacidad de identificar Exploits en documentos y archivos de Office.
2.4	La solución deberá tener Sandbox para análisis de amenazas desconocidas y ataques de día cero.
2.5	La solución deberá ofrecer un análisis de riesgo para reducir el impacto en los usuarios
2.6	La solución deberá tener escaneo de URL en el cuerpo de los correos y en los archivos adjuntos.
2.7	La solución deberá ofrecer protección avanzada contra amenazas para OneDrive, SharePoint, Teams.
2.8	La solución debe tener una capacidad de protección colaborativa para detectar archivos maliciosos que se encuentran en SharePoint, OneDrive, Teams.
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
2.10	La solución deberá tener DLP a nivel de Email con la capacidad de descubrir y reportar violaciones a las políticas.
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.
2.12	La solución deberá ofrecer disponibilidad del servicio superior a >99%.
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).
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.
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.
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
2.17	La solución deberá tener la capacidad en la consola en la nube de reportar ataques dirigidos.
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.
2.19	La solución debe proporcionar seguridad para la información que se encuentra almacenada en la nube y garantizar la privacidad de la misma.
2.20	La solución debe tener la capacidad de identificar amenazas que aún no han sido reportadas con el análisis de los archivos.
2.21	La solución debe proporcionar protección contra ataques de BEC (Business Email Compromise – Compromiso en cuentas corporativas) con el análisis de los mensajes.
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

ÍTEM	DESCRIPCIÓN
2.23	La solución debe contar con la capacidad de tener una funcionalidad de inteligencia correlacionada
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
2.25	La solución debe tener la capacidad de detectar ataques dirigidos mediante explotación de archivos.
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.
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.
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.
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.
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.
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.
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.
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
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.
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.
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.
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.
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.
2.39	La solución debe soportar la extracción de URL de códigos QR para detener ataques de phishing, ransomware y BEC.

ÍTEM	DESCRIPCIÓN
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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
3.2	La solución puede distinguir el acceso a funciones y parámetros según los roles.
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
4.2	La solución debe poder notificar a un destinatario interno en caso de correo electrónico en cuarentena / eliminado / limpiado
4.3	La solución debe poder enviar eventos de alerta por correo electrónico al SIEM QRadar
5.	**REPORTES**
5.1	La solución debe conservar los registros (usuario y 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.
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.

ÍTEM	DESCRIPCIÓN
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.
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.
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.
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.
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).
6.7	Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.
6.8	XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.
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
6.10	Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el fabricante
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.
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.
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.
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.
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.
6.16	La solución debería tener la capacidad de eliminar el mensaje de correo electrónico seleccionado de los buzones seleccionados.
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.
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
7.2	El fabricante debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos.
7.3	Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).
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.
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

ÍTEM	DESCRIPCIÓN
	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
7.7	Los modelos deben especificar la última vez que se actualizó
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.
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.
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:
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.
10.	**GESTIÓN 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.
10.2	La solución debe proporcionar una plataforma centralizada de visibilidad y gestión en soluciones de correo electrónico basadas en API y gateway.
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
10.4	Debe poder identificar a los usuarios más específicos de la organización y configurar políticas de acceso condicional para los usuarios riesgosos.
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.
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.
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.
10.8	La solución debe ofrecer una integración de detección y respuesta de correo electrónico (Email DR) y Gestión de exposición de Riesgos

ÍTEM	DESCRIPCIÓN
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
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.
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.
11.3	La solución debería ofrecer una opción para ampliar la retención de datos hasta 365 días.
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)
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.
12.2	La solución debe poder integrarse con productos SIEM y SOAR comunes.
12.3	La solución debe poder integrarse con soluciones IdP de terceros para los requisitos de inicio de sesión único (SSO).
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.
12.5	La solución también debe tener la capacidad de integrarse con otras soluciones de terceros a través de API.
12.6	La solución debe proporcionar conectores listos para integrarse con otras soluciones de seguridad de terceros compatibles
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
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.
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.

ÍTEM	DESCRIPCIÓN
	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.
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.
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.
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.
13.6	La solución debe poder gestionar todos los activos descubiertos desde una única consola de gestión unificada.
13.7	La solución debe poder integrarse con proveedores externos para incorporar o enriquecer datos de la superficie de ataque.
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).
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.
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.
13.11	La solución debe ser capaz de modificar la criticidad de un activo en función de la necesidad de la compañía.
13.12	La solución debe tener soporte integrado para manuales de seguridad que puedan usarse para la remediación automatizada.
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).
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.
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.
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.

ÍTEM	DESCRIPCIÓN
13.17	Debe utilizar múltiples proveedores de datos de descubrimiento (la dependencia del agente existente 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.
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.
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.
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.
13.22	Los informes se pueden generar por demanda o mediante programación.
13.23	El contenido de los informes se puede filtrar para limitar la salida según criterios seleccionados
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).
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.
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 • 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
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.

ÍTEM	DESCRIPCIÓN
	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 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.
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) -

ÍTEM	DESCRIPCIÓN
	- **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.
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
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).
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.
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.
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.
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.
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.
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 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

ÍTEM	DESCRIPCIÓN
	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.
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.
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.
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.
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.
20.7	El contratista garantizará que el personal que ingrese a las instalaciones se encuentre con la debida identificación de la empresa.
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.
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.
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.
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

ÍTEM	DESCRIPCIÓN
	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.
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.
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.
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.
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.

LA DIRECCIÓN DE INTELIGENCIA POLICIAL

Brigadier general **RICARDO SÁNCHEZ SILVESTRE**
Director de Inteligencia Policial

CONTRATISTA

Laura Marcela Cepeda S

LAURA MARCELA CEPEDA SANABRIA
Representante Legal: HIGH TECH SERVICES CORP (HTS CORP) S.A.S.

Elaboró IJ. Edison Alexander Gutiérrez González Analista de contratos	Vo. Bo. / SI. Deyri Daniela Duarte Duarte Sustanciador	Vo. Bo. / MY. Pedro David Mondragón Piñeros Jefe Grupo de Contratos
Vo. Bo. / MY. Alexander Malagón Aguillón Jefe Grupo Asuntos Jurídicos	Vo. Bo. / TC. Henry Giovanny Sánchez Holguín Jefe Área Logística y Financiera	Vo. Bo. / CR. José Manuel Álvarez Omaña Subdirector de Inteligencia Policial