No. GS-2026-039124 - DIPOL

Bogotá D.C., 19/09/2026

Brigadier general
RICARDO SÁNCHEZ SILVESTRE
Director de Inteligencia Policial
Avenida Boyacá 142ª-55
Bogotá D.C

ASUNTO: informe final del contrato No. 04-2-10024-2026

TIPO DE INFORME

PERIÓDICO __ O FINAL _X_

Desde	25-05-2026	Hasta	10-08-2026

En cumplimiento a los artículos 83 y 84 de la Ley 1474 de 2011 "*Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública*", así como de la Resolución No.03049 del 30 de julio del 2014 "*Por la cual se adopta el Manual de Contratación de la Policía Nacional*", Resolución No. 00090 del 15/01/2018, "*Por la cual se actualiza, modifica y complementa el Manual de Contratación de la Policía Nacional adoptado mediante Resolución No. 03049 de 2014*", y la "*Guía para el ejercicio de las funciones de Supervisión e Interventoría de los contratos del Estado*" expedida por Colombia Compra Eficiente, o las normas que las modifiquen, adicionen o sustituyan, sin perjuicio de las funciones establecidas contractualmente y aquellas inherentes a la naturaleza del ejercicio de la supervisión, me permito presentar el correspondiente informe del contrato u orden de compra del asunto a través del cual se detalla, el seguimiento y el grado de cumplimiento de las obligaciones establecidas en el respectivo contrato u orden, así:

INFORMACIÓN GENERAL:

Mediante comunicación oficial No. GS-2026-021388-DIPOL del 25/05/2026, el señor mayor Pedro David Mondragon Piñeros obrando en calidad de jefe Grupo Contratos DIPOL, notificó como supervisora del contrato No. 04-2-10024-2026 a la señora capitán Yenny Marcela Corredor Cristancho, jefe del Centro Protección de Datos.

- **Periodicidad establecida para la entrega del informe de supervisión:** mensual
- **No. de informes de supervisión presentados y publicados en SECOP II: 3**

1. Informe de supervisión del mes de mayo del periodo comprendido entre el 25/05/2026 y el 24/06/2026, presentado mediante comunicación oficial No. GS-2026-026432-DIPOL del 25/06/2026.

2. Segundo informe de supervisión del mes de mayo del periodo comprendido entre el 25/06/2026 y el 24/07/2026, presentado mediante comunicación oficial No. GS-2026-030458-DIPOL del 24/07/2026.

3. Tercer informe de supervisión del mes de agosto del periodo comprendido entre el 25/07/2026 y el 10/08/2026, presentado mediante comunicación oficial No. GS-2026-033357-DIPOL del 12/08/2026.

Información del contrato u orden de compra

Contrato No. / Orden de compra No.	04-2-10024-2026
Objeto del Contrato / instrumento de agregación de la orden de compra	ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL
Contratista	HIGH TECH SERVICES CORP (HTS CORP) S.A.S.
Representante legal	LAURA MARCELA CEPEDA SANABRIA
Valor inicial del contrato u orden de compra	$277.799.900,00
Valor adiciones del contrato u orden de compra	N/A
Valor total del contrato u orden de compra	$277.799.900,00
Plazo de ejecución inicial	10-08-2026
Fecha de inicio del plazo de ejecución del contrato u orden de compra	25-05-2026
Fecha de terminación del plazo de ejecución del contrato u orden de compra (pactada inicialmente)	10-08-2026
Fecha de inicio del plazo de ejecución de la(s) adición(es)	N/A
Fecha de terminación del plazo de ejecución de la(s) adición(es)	N/A
Adiciones	N/A
Modificatorios	N/A
Prorrogas	N/A
Otros	N/A

1. DESARROLLO DE LA SUPERVISIÓN AL CONTRATO U ORDEN DE COMPRA

1.1 Acciones adelantadas:

- Mediante el acta No. 103 – DIPOL-CPD del 26/05/2026, se realizó reunión con el contratista con el fin de dar inicio formal del contrato No. 04-2-10024-2026 correspondiente a "ADQUISICIÓN LICENCIAMIENTO PARA LA PROTECCIÓN DE CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN EN LA NUBE PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL".

- Para el 03/06/2026 se recibió correo electrónico por parte del fabricante, en el cual remitieron la carta de titularidad del licenciamiento con número SKUVONA0000 y número de licencia COL 160738 para cuatrocientas (400) cuentas de correo electrónico.

- Para el 04/06/2026 se realizó activación de consola de administración donde a su vez se cargó el licenciamiento adquirido quedando a espera de integración con la infraestructura de DIPOL ya que conforme lo manifestado con el grupo de Tecnologías de la Información y las Comunicaciones no es posible aprobar cambios en la infraestructura de la DIPOL durante el periodo previo a las elecciones presidenciales, por lo que se procedió a documentar caso sigma de numero **DIPOL-2026-8163** para el control de cambios posterior al 21 de junio de 2026.

- Con el propósito de asegurar el cumplimiento a los controles de seguridad de la información y los requisitos establecidos para el proceso de direccionamiento tecnológico, en comité de control de cambios

se generó concepto de viabilidad por parte del Grupo Tecnologías de la Información y las Comunicaciones – DIPOL, mediante Acta 112 DIPOL-GUTIC del 26 de junio de 2026, para realizar la implementación de la herramienta de protección para correo y herramientas colaborativas de nube TREND VISION ONE en la plataforma tecnológica de la Dirección de Inteligencia Policial, en aras de fortalecer el componente tecnológico en materia de protección de datos y seguridad de la información.

- El día 22/06/2026 se recibe por correo electrónico de la empresa HIGH TECH SERVICES CORP S.A.S, donde anexan documento relacionado con: procedimiento de gestión de tickets, escalamiento al fabricante, carta de distribuidor autorizado y disponibilidad de base de conocimiento para soporte técnico.

- El contratista en el trascurso de la ejecución contractual, ha realizado las actividades correspondientes a la implementación de la solución tecnológica Trend Vision One, en sitio, con personal capacitado, idóneo y autorizado, con el acompañamiento de personal de CPD y GUTIC – DIPOL, donde se realizaron las siguientes actividades:

  Para la semana comprendida del 30 de junio al 03 de julio de 2026, se contó con la presencia de 01 ingeniero de soporte de la empresa HIGH TECH SERVICES CORP S.A.S donde se ejecutaron las siguientes actividades descritas en el cronograma del acta de inicio y los cuales se encuentran documentados en los respectivos informes.

  Para la semana comprendida del 04 al 09 de julio de 2026, se contó con la presencia de 01 ingeniero de soporte de la empresa HIGH TECH SERVICES CORP S.A.S donde se ejecutaron las siguientes actividades descritas en el cronograma del acta de inicio y los cuales se encuentran documentados en los respectivos informes.

  Como parte de las actividades de implementación, se realizaron las validaciones funcionales y técnicas de las capacidades de la solución TrendIA Vision One, verificando la operación de cada uno de los componentes e integraciones requeridas. Los resultados de las pruebas, configuraciones y afinamientos ejecutados quedaron documentados y soportados mediante evidencias descriptivas, capturas de pantalla y pruebas ejecutadas en la consola de gestión de producción.

- El día 06/07/2026, mediante comunicación oficial GS-2026-028242-DIPOL suscrita por el Área de Contrainteligencia, se informan los resultados obtenidos del estudio de credibilidad y confiabilidad para los ingenieros y terceros de la empresa HIGH TECH SERVICES CORP S.A.S que realizarán las actividades de soporte técnico e implementación de la herramienta de protección para correo y herramientas colaborativas de nube TREND VISION ONE.

- El contratista hizo entrega del certificado de autenticidad, certificado de la licencia emitido por el fabricante, documentos que permitieron iniciar el trámite de ingreso de la licencia al inventario tecnológico de la DIPOL (sistemas SINVE y SILOG), mediante la comunicación oficial GS-2026-027816-DIPOL, el almacenista de GUTIC generó el Acta No. 005 del 07 de julio de 2026, confirmando la recepción e ingreso al inventario de la licencia.

- El día 10 de julio, la empresa hace entrega de los documentos que soportan todas las actividades ejecutas en la implementación la herramienta de protección para correo y herramientas colaborativas de nube TREND VISION ONE en la infraestructura tecnológica de DIPOL.

- Para los días 14 y 15 de julio de 2026, se llevó a cabo la transferencia de conocimiento en la administración de la herramienta de protección para correo electrónico y herramientas colaborativas de nube TREND VISION ONE, donde se contó con la participación de 03 funcionarios del CPD y 02 funcionario de GUTIC, capacitación orientada a la configuración y administración técnica y funcional de la solución. Capacitación orientada por el personal de ingenieros de soporte de la empresa HIGH TECH

SERVICES CORP S.A.S y el acompañamiento permanente de ingenieros de casa fabricante, donde la empresa entrega los certificados de asistencia.

- El 15/07/2026 se presentó la constancia de recibo a satisfacción de bienes o servicios, correspondiente al período comprendido entre el 25/05/2026 y el 15/07/2026, para efectos de tramitar el pago equivalente al 100% del valor total del contrato, certificando el cumplimiento de las obligaciones contractuales.

- Para el 02 de agosto de 2026, le fue notificado a la empresa HTS, el pago de la factura FE1135, que la orden de pago fue exportada directamente del aplicativo y discrimina los descuentos por impuestos que fueron afectados en la obligación (concepto y valor), en cumplimiento al Decreto 019 de 2012 "ARTÍCULO 28. COMPROBANTES DE DESCUENTOS Y RETENCIONES: Las entidades públicas y las privadas que cumplan funciones administrativas o presten servicios públicos que paguen o abonen en cuenta a favor de cualquier persona una obligación a su cargo deberán certificar los descuentos o las retenciones que le hayan sido practicados al beneficiario con indicación precisa de la norma legal con que se haya procedido. Para tal efecto, podrán enviar la certificación a la dirección electrónica que haya registrado el beneficiario e impuestos.

Seguimiento pólizas de garantía:

Dando cumplimiento de las actividades de supervisión ordenadas en la comunicación oficial GS-2026-022096-DIPOL, durante el periodo reportado en el presente informe se adelantaron las siguientes actividades de control sobre las garantías del contrato, así:

- **Revisión vigencia:** Se verificó que la Garantía Única No. 11-44-101283410, emitida por la aseguradora Seguros del Estado S.A, mantiene su vigencia y suficiencia económica, cubriendo el 100% de los riesgos contractuales vigentes hasta el 10/12/2029.

- **Novedades presentadas:** Durante el periodo de supervisión contractual no se presentaron modificaciones que alteraran el plazo o valor del contrato, por lo cual la póliza se mantiene sin cambios.

- **Cumplimiento del contrato:** A la fecha del presente informe, el amparo de cumplimiento cubre la totalidad del plazo de ejecución contractual y los meses adicionales requeridos por la entidad. No se han presentado siniestros ni retrasos que afecten la vigencia de la garantía.

- **Verificación de pagos:** Se verificó que el contratista se encuentra al día con el pago de pago de salarios, prestaciones e indemnizaciones laborales, con el fin de evitar la terminación automática del contrato de seguro.

- **Calidad bienes:** Se certifica que los bienes adquiridos durante el periodo reportado, cumplen a satisfacción con las fichas técnicas y estándares establecidos, sin presentar fallas a la fecha.

2. VERIFICACIÓN DEL CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES

CUMPLIMIENTO OBLIGACIONES LEGALES DEL CONTRATISTA

ITEM	OBLIGACIONES DEL CONTRATISTA LEGALES	CUMPLIÓ	OBSERVACIONES
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	SI	La empresa entregó los documentos donde se evidenció el número de trabajadores permanentes y el nivel de riesgo

	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 Mínimos del Sistema de Gestión de SST en el marco del Sistema de Garantía de Calidad del Sistema General de Riesgos Laborales.		de su principal actividad económica.
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.	SI	La empresa entregó los documentos donde se evidenció objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual planilla No. 93172618 (E.P.S., A.F.P, A.R.L., C.C.F.).
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.	SI	Durante la ejecución del contrato no se presentaron accidentes de trabajo dentro de las instalaciones de DIPOL.
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.	SI	El contratista no presentó ningún incidente respecto a hospitalización y procedimientos médicos.
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.	SI	El contratista garantizo que el personal que dio soporte en las instalaciones de la DIPOL, cumpliera con las orientaciones del personal profesional en caso de presentarse emergencias.
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.	SI	Durante la ejecución del contrato no se presentaron auditorías del SG-SST. Sin embargo, el contratista manifestó su disposición de entregar la documentación en caso de ser requerida.

20.7	El contratista garantizará que el personal que ingrese a las instalaciones se encuentre con la debida identificación de la empresa.	SI	El contratista ha cumplido con el ítem especificado, teniendo en cuenta que el ingeniero que brinda soporte técnico en las instalaciones de la Dirección de Inteligencia Policial cuenta con la identificación suministrada por 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.	SI	Hasta el momento el contratista ha cumplido con la aplicación de las buenas prácticas ambientales establecidas por la dirección
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.	SI	Hasta el momento se ha cumplido con la aplicación de la normatividad ambiental vigente.
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.	SI	Tanto el representante legal de la empresa, como los ingenieros de soporte suscribieron compromiso de reserva, así mismo el día 06/07/2026, mediante comunicación oficial GS-2026-028242-DIPOL suscrita por el Área de Contrainteligencia, se informan los resultados obtenidos del estudio de credibilidad y confiabilidad.
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	SI	Se realizó el diligenciamiento del formato declaración de confidencialidad y compromiso con la seguridad de la información, por parte del representante legal y los ingenieros que se encuentran desarrollando las actividades objeto del contrato.

	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.	SI	Se realizó el diligenciamiento del formato declaración de confidencialidad y compromiso con la seguridad de la información, así como del compromiso de reserva, por parte del representante legal y los ingenieros que se encuentran desarrollando las actividades objeto del contrato
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.	SI	Se realizó el diligenciamiento del formato declaración de confidencialidad y compromiso con la seguridad de la información, así como del compromiso de reserva, por parte del representante legal y los ingenieros que se encuentran desarrollando las actividades objeto del contrato.
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.	SI	Se realizó el diligenciamiento del formato declaración de confidencialidad y compromiso con la seguridad de la información, así como del compromiso de reserva, por parte del representante legal y los ingenieros que se encuentran en desarrollo del soporte técnico.
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.	SI	Tanto el representante legal de la empresa, como los ingenieros de soporte suscribieron compromiso de reserva, así mismo el día 06/07/2026, mediante comunicación oficial GS-2026-028242-DIPOL suscrita por el Área de Contrainteligencia, se informan los resultados obtenidos del estudio de credibilidad y confiabilidad.

CUMPLIMIENTO ESPECIFICACIONES TÉCNICAS

ITEM	CONDICIONES TÈCNICAS MINIMAS	CUMPLIÓ	OBSERVACIONES
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.	SI	La empresa entregó certificado de titularidad del licenciamiento de la marca Trend AI y referencia TrendAI Vision One para

			cuatrocientas (400) cuentas de correo electrónico.
1.2	**MARCA:** Trend AI **REFERENCIA:** TREND VISION ONE **FABRICANTE:** Trend Micro Incorporated	SI	La empresa entregó certificado de titularidad del licenciamiento de la marca Trend AI y referencia TrendAI Vision One para cuatrocientas (400) cuentas de correo electrónico.
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	SI	La solución tecnológica TrendAI Vision One, cuenta con la capacidad de proteger la plataforma de Microsoft Office 365 de la DIPOL.
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	SI	La solución tecnológica TrendAI Vision One, cuenta con la capacidad de proteger la plataforma de Microsoft Office 365 de la DIPOL de distintos dominios.
2.3	La solución deberá tener motores para la detección de malware con la capacidad de identificar Exploits en documentos y archivos de Office.	SI	La solución tecnológica TrendAI Vision One, cuenta con motores para la detección de malware ocultos en documentos y archivos de Office.
2.4	La solución deberá tener Sandbox para análisis de amenazas desconocidas y ataques de día cero.	SI	La solución tecnológica TrendAI Vision One, cuenta con funcionalidades de Sandbox para el 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	SI	La solución tecnológica TrendAI Vision One, cuenta con funcionalidades de análisis de riesgos que permiten identificar y mitigar amenazas, contribuyendo a 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.	SI	La solución tecnológica TrendAI Vision One, cuenta con funcionalidades de escaneo de URL en el cuerpo de los correos electrónicos y en los archivos adjuntos.
2.7	La solución deberá ofrecer protección avanzada contra amenazas para OneDrive, SharePoint, Teams.	SI	La solución tecnológica TrendAI Vision One, cuenta con protección avanzada contra amenazas para OneDrive, SharePoint y Microsoft Teams.
2.8	La solución debe tener una capacidad de protección colaborativa para detectar archivos maliciosos que se encuentran en SharePoint, OneDrive, Teams.	SI	La solución tecnológica TrendAI Vision One, cumple con el requisito, al disponer de protección colaborativa para SharePoint, OneDrive y Microsoft Teams.
2.9	La solución deberá tener plantillas personalizables de DLP para controlar la fuga de información permitiendo realizar pruebas de	SI	La solución tecnológica TrendAI Vision One, permitió la personalización de plantillas DLP

	expresiones regulares y listados de palabras para nuevas plantillas		mediante diccionarios de detección definidos por la DIPOL.
2.10	La solución deberá tener DLP a nivel de Email con la capacidad de descubrir y reportar violaciones a las políticas.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la personalización de políticas DLP para correo electrónico, facilitando la detección y el reporte de violaciones a las políticas de seguridad definidas por la DIPOL.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al contar con la funcionalidad DLP para SharePoint, OneDrive y Microsoft Teams.
2.12	La solución deberá ofrecer disponibilidad del servicio superior a >99%.	SI	El servicio es superior a un >99% de disponibilidad del proveedor de nube. https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-service-level-objectives
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).	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al contar con una consola de gestión en la nube que permite crear y administrar políticas para correos entrantes y salientes, con acciones configurables como limpiar, eliminar, etiquetar (tag), cifrar y 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al contar con una consola de gestión en la nube que permite visualizar gráficos e indicadores para el seguimiento del tráfico de correo electrónico y la administración de 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir desde la consola de administración de la nube cambiar que los usuarios finales gestionen remitentes confiables y aprueben correos en cuarentena según las políticas definidas.
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,	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al contar con capacidades de análisis de enlaces en el cuerpo de los

	ya sea en botones, banners o imágenes en el momento en el que el usuario le dé clic en el enlace		correos electrónicos, incluyendo URL ocultas en botones, banners e imágenes, verificándolas en el momento en que el usuario accede a ellas
2.17	La solución deberá tener la capacidad en la consola en la nube de reportar ataques dirigidos.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al contar con una consola de administración en la nube que permite identificar y reportar ataques mediante paneles, alertas e información detallada.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, permitiendo la aplicación de políticas y reglas de forma granular sobre usuarios específicos y elementos específicos del correo electrónico.
2.19	La solución debe proporcionar seguridad para la información que se encuentra almacenada en la nube y garantizar la privacidad de la misma.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al proporcionar protección para la información almacenada en la nube y contribuir a garantizar su privacidad.
2.20	La solución debe tener la capacidad de identificar amenazas que aún no han sido reportadas con el análisis de los archivos.	SI	El sandbox integrado en la consola de gestión tiene la capacidad de analizar amenazas nuevas que aún no han sido reportadas.
2.21	La solución debe proporcionar protección contra ataques de BEC (Business Email Compromise – Compromiso en cuentas corporativas) con el análisis de los mensajes.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al proporcionar protección contra ataques de Business Email Compromise (BEC) mediante el análisis avanzado de mensajes de correo electrónico.
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	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al contar con capacidades de análisis basadas en inteligencia artificial para identificar anomalías en el estilo de escritura y detectar intentos de Business Email Compromise (BEC) dirigidos a usuarios de alto perfil.
2.23	La solución debe contar con la capacidad de tener una funcionalidad de inteligencia correlacionada	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al disponer de inteligencia correlacionada para la visualización y análisis de relaciones entre eventos de seguridad.

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	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la evaluación reputacional de URL y el bloqueo de acceso a sitios web maliciosos.
2.25	La solución debe tener la capacidad de detectar ataques dirigidos mediante explotación de archivos.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al detectar ataques dirigidos mediante el análisis avanzado 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al utilizar Machine Learning para la identificación de amenazas desconocidas en archivos.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al brindar protección contra BEC, ransomware, phishing y otras amenazas avanzadas.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir eliminar, poner en cuarentena, liberar y etiquetar correos identificados como spam.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir poner en cuarentena, eliminar, etiquetar o liberar correos analizados por Sandbox e identificados como maliciosos o sospechosos.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir poner en cuarentena, eliminar o liberar archivos identificados como maliciosos o sospechosos, notificando al usuario sobre la acción ejecutada.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al notificar al usuario la acción aplicada sobre el correo y la razón de dicha acción.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al mantener sincronizada y actualizada la lista de objetos sospechosos desde 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	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, ya que permitió la

	administrar la consola usando las credenciales registradas en estos servicios		integración con Microsoft Azure AD para la gestión y autenticación de usuarios administradores.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, ya que permitió la integración con IBM QRadar, Palo Alto, Fortinet y Directorio Activo, para el intercambio de información de seguridad y el fortalecimiento de la postura de riesgo.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la configuración de excepciones para archivos detectados por Machine Learning.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la restauración de archivos enviados a cuarentena.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la evaluación de políticas sin afectar correos ni 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al utilizar tecnología de reputación web para analizar URL y bloquear enlaces maliciosos o sospechosos.
2.39	La solución debe soportar la extracción de URL de códigos QR para detener ataques de phishing, ransomware y BEC.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al analizar URL contenidas en códigos QR para detectar y bloquear amenazas de phishing, ransomware y BEC.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al realizar análisis dinámico de URL en tiempo real para detectar y bloquear amenazas 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al utilizar inteligencia artificial y visión computacional para detectar sitios de phishing que imitan marcas legítimas.

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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al utilizar inteligencia artificial y visión artificial para identificar formularios de autenticación fraudulentos y prevenir el robo de credenciales.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al disponer de políticas y plantillas DLP para correo electrónico y servicios de colaboración en la nube, incluyendo SharePoint, OneDrive y Microsoft Teams.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al correlacionar eventos de correo electrónico con identidad, endpoints, red y otros vectores mediante capacidades XDR.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al disponer de modelos de detección predefinidos basados en Machine Learning y actualizaciones continuas para mejorar la detección de amenazas.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir al administrador de la solución habilitar, deshabilitar y personalizar modelos de detección, así como definir excepciones según las necesidades de la DIPOL.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir al administrador personalizar modelos de detección y filtros de eventos para la generación de 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al identificar ataques en curso mediante el análisis y correlación de indicadores de seguridad, apoyando las actividades de investigación y respuesta del SOC.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al mapear eventos de seguridad al marco MITRE

			ATT&CK para facilitar las investigaciones del SOC.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al correlacionar eventos de seguridad con las TTP del marco MITRE ATT&CK para fortalecer el análisis e investigación de amenazas.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir al administrador crear, guardar y ejecutar consultas personalizadas sobre la telemetría de seguridad, facilitando el seguimiento continuo de eventos e indicadores.
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	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la administración de accesos a la consola mediante roles y permisos diferenciados.
3.2	La solución puede distinguir el acceso a funciones y parámetros según los roles.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la creación de usuarios con roles diferenciados y acceso específico a funciones y parámetros según su perfil.
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	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir al administrador definir umbrales de notificación para reducir la generación de alertas innecesarias.
4.2	La solución debe poder notificar a un destinatario interno en caso de correo electrónico en cuarentena / eliminado / limpiado	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al notificar a los usuarios internos las acciones de cuarentena, eliminación o limpieza aplicadas a los correos electrónicos.
4.3	La solución debe poder enviar eventos de alerta por correo electrónico al SIEM QRadar.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al encontrarse integrada con IBM QRadar y remitir correctamente eventos de seguridad para su correlación en la plataforma SIEM.
5.	**REPORTES**		
5.1	La solución debe conservar los registros (usuario y administrador) durante al menos 3 meses	SI	La solución tecnológica TrendAI Vision One cumple con el

			requisito, al mantener los registros de usuarios y administradores por un período mínimo de tres (3) meses según necesidades de los administradores.
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.	SI	La solución tecnológica TrendAI Vision One, tiene paneles de control que permiten visualizar métricas de correos analizados, amenazas detectadas, niveles de riesgo y estadísticas de seguridad.
6.	**CAPACIDADES DE DETECCCIÓN 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al disponer de modelos de detección XDR que correlacionan eventos de diferentes capas de seguridad para identificar ataques avanzados.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al contar con modelos de correlación que integran múltiples reglas y filtros, apoyados en tecnologías avanzadas de análisis, incluyendo Machine Learning y correlación de eventos para la identificación de amenazas.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir al administrador activar o desactivar modelos de detección XDR según los requerimientos de seguridad de la DIPOL.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al proporcionar una interfaz visual de investigación que correlaciona automáticamente eventos de seguridad, inteligencia de amenazas y técnicas MITRE ATT&CK, permitiendo analizar el impacto sobre los activos comprometidos y las actividades asociadas a un incidente
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir visualizar el análisis de causa raíz de las alertas, identificar el impacto del

			incidente y ejecutar 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).	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la priorización de alertas, el seguimiento de su estado y el registro de las acciones ejecutadas durante su atención.
6.7	Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al proporcionar una visualización gráfica de los objetos involucrados en una alerta y su relación dentro del incidente.
6.8	XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir visualizar de forma gráfica e interactiva la historia del ataque y la relación entre los eventos asociados al incidente.
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	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir consultar el perfil de ejecución y el análisis de causa raíz de amenazas detectadas en correos de Office 365
6.10	Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el fabricante	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al realizar búsquedas automáticas de IoC proporcionados por el fabricante para la detección proactiva de amenazas.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al identificar campañas de amenazas, plataformas afectadas y TTP asociados al marco MITRE ATT&CK, proporcionando contexto adicional e información de inteligencia para su análisis.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al incorporar un chatbot basado en inteligencia artificial que asiste a los analistas en investigaciones y consultas de 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir la gestión de IoC mediante la adición y eliminación de dominios, URL,

			direcciones IP y hashes de archivos desde la consola de administración.
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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al integrar protección para correo electrónico y servicios de colaboración, enriquecida con capacidades XDR y 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.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir poner en cuarentena mensajes de correo electrónico y aplicar la acción sobre todos los buzones afectados.
6.16	La solución debería tener la capacidad de eliminar el mensaje de correo electrónico seleccionado de los buzones seleccionados.	SI	La solución tecnológica TrendAI Vision One cumple con el requisito, al permitir eliminar mensajes de correo electrónico de los buzones seleccionados desde la consola de administración.
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.	SI	La solución tecnológica TrendAI Vision One, permite realizar búsqueda y filtrado que facilitan la identificación y consulta de eventos, alertas y objetos de seguridad.
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	SI	La solución tecnológica TrendIA Vision One, integra el marco MITRE ATT&CK en sus modelos de detección, relacionando las alertas con tácticas y técnicas para el análisis de amenazas.
7.2	El fabricante debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos.	SI	La solución tecnológica TrendIA Vision One cuenta con actualizaciones y mejoras continuas en los modelos de detección y filtros, optimizando la detección de amenazas y reduciendo la generación de falsos positivos.
7.3	Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).	SI	La solución tecnológica TrendIA Vision One, prioriza los incidentes mediante puntajes de riesgo (Risk Score), facilitando la toma de decisiones y la atención de eventos críticos.
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	SI	La solución tecnológica TrendIA Vision One, permite al administrador gestionar alertas y configurar criterios de notificación según la criticidad y categoría de las amenazas.

	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 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).	SI	La solución tecnológica TrendIA Vision One, permite clasificar los eventos detectados en niveles de severidad (Crítico, Alto, Medio y Bajo), facilitando su priorización y atención por parte del equipo de seguridad.
7.6	Los modelos deben especificar y permitir modificar el estado: encendido/apagado	SI	La solución tecnológica TrendIA Vision One, permite cambiar el estado de los modelos de detección entre habilitado y deshabilitado según las necesidades de la organización
7.7	Los modelos deben especificar la última vez que se actualizó	SI	La solución tecnológica TrendIA Vision One, muestra la fecha y hora de la última actualización de cada modelo de detección en la consola de administración.
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.	SI	La solución tecnológica TrendIA Vision One, ya que permite el envío de alertas mediante Webhooks y su configuración según niveles de severidad.
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.	SI	La solución tecnológica TrendIA Vision One cumple, permite ejecutar acciones de respuesta automatizada como cuarentena de correos, cierre forzado de sesiones y restablecimiento de contraseñas, entre otras.
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:	SI	La solución tecnológica TrendIA Vision One, permite la gestión de usuarios, roles, autenticación, API Keys, auditoría e integración de servicios adicionales desde la consola XDR.
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.	SI	La solución tecnológica TrendIA Vision One, proporciona capacidades de SSO, gestión de usuarios y roles, conectores nativos, registros de auditoría y acceso controlado para soporte remoto del fabricante.

	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.	SI	La solución tecnológica TrendIA Vision One, integra la protección de correo electrónico mediante API, Inline Mode y Gateway en una única plataforma de gestión.
10.2	La solución debe proporcionar una plataforma centralizada de visibilidad y gestión en soluciones de correo electrónico basadas en API y gateway.	SI	La solución tecnológica TrendIA Vision One, integra en una única consola la gestión y visibilidad de las 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	SI	La solución tecnológica TrendIA Vision One, permite visualizar las cuentas de correo electrónico y los dominios de la organización desde una consola centralizada.
10.4	Debe poder identificar a los usuarios más específicos de la organización y configurar políticas de acceso condicional para los usuarios riesgosos.	SI	La solución tecnológica TrendIA Vision One, permite definir usuarios de alto riesgo y aplicar controles de seguridad diferenciados según su nivel de exposición.
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.	SI	La solución tecnológica TrendIA Vision One, permite la automatización de tareas de seguridad mediante playbooks y flujos de trabajo que aceleran las actividades de respuesta e investigación.
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.	SI	La solución tecnológica TrendIA Vision One, soporta Microsoft Information Protection (MIP) para el análisis de correos electrónicos y archivos protegidos en los servicios de Microsoft 365.
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.	SI	La solución tecnológica TrendIA Vision One, permite la personalización de paneles mediante widgets para visualizar estadísticas de superficie de ataque, correo electrónico, identidades y otros indicadores de seguridad.
10.8	La solución debe ofrecer una integración de detección y respuesta de correo electrónico (Email DR) y Gestión de exposición de Riesgos	SI	La solución tecnológica TrendIA Vision One, cuenta con capacidades de Email Detection and Response (Email DR) y gestión de exposición al riesgo para la detección, análisis y

			mitigación de amenazas de seguridad.
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	SI	La solución tecnológica TrendIA Vision One, cuenta con tableros que muestran el mapeo MITRE ATT&CK para las matrices Enterprise, Mobile e 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.	SI	La solución tecnológica TrendIA Vision One, permite realizar análisis de causa raíz, investigar el perfil de ejecución de los ataques e identificar el impacto sobre los activos desde una consola unificada.
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.	SI	La solución tecnológica TrendIA Vision One, permite conservar alertas y registros históricos por un período igual o superior a 180 días, permitiendo su consulta e investigación desde la consola.
11.3	La solución debería ofrecer una opción para ampliar la retención de datos hasta 365 días.	SI	La solución tecnológica TrendIA Vision One, permite la ampliación de la retención de datos hasta 365 días y la consulta de información histórica mediante períodos personalizados.
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)	SI	La solución tecnológica TrendIA Vision One cumple con el requisito, toda vez que fueron entregados los soportes que acreditan las certificaciones ISO 27001, ISO 27014, ISO 27017 y SOC 2/SOC 3 del fabricante.
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.	SI	La solución tecnológica TrendIA Vision One, soporta la integración con Microsoft Information Protection (MIP) para el descifrado y análisis de correos electrónicos y archivos protegidos.
12.2	La solución debe poder integrarse con productos SIEM y SOAR comunes.	SI	La solución tecnológica TrendIA Vision One, permite integrarse con plataformas SIEM y SOAR mediante conectores nativos que

			permiten compartir eventos, alertas y acciones de respuesta de seguridad.
12.3	La solución debe poder integrarse con soluciones IdP de terceros para los requisitos de inicio de sesión único (SSO).	SI	La solución tecnológica TrendIA Vision One, soporta integración con proveedores de identidad (IdP) mediante SAML para habilitar el 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.	SI	La solución tecnológica TrendIA Vision One, permite la creación de claves API asociadas a roles específicos, con opciones de caducidad y desactivación 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.	SI	La solución tecnológica TrendIA Vision One, permite la integración con soluciones de terceros mediante API, gestionando de forma granular los permisos, roles y vigencia de las credenciales de acceso.
12.6	La solución debe proporcionar conectores listos para integrarse con otras soluciones de seguridad de terceros compatibles	SI	La solución tecnológica TrendIA Vision One, cuenta con conectores nativos para la integración con 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	SI	La solución tecnológica TrendIA Vision One, fue integrada con Firewall Fortinet, Firewall Palo Alto, SIEM IBM QRadar y Directorio Activo, además de soportar integraciones adicionales con otras tecnologías de terceros.
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.	SI	La solución tecnológica TrendIA Vision One, integra correlación de telemetría, evaluación de riesgos, visibilidad de la superficie de ataque y puntuación contextualizada para la gestión integral del riesgo cibernético.
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	SI	La solución tecnológica TrendIA Vision One, integra inteligencia de amenazas basada en ZDI, priorizar vulnerabilidades según su nivel de explotación real, correlacionar intentos de ataque y detectar configuraciones incorrectas en diferentes plataformas.

	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.	SI	La solución tecnológica TrendIA Vision One, ofrece recomendaciones de mitigación, playbooks de respuesta automatizada, integración con soluciones de seguridad de terceros, personalización de reglas de riesgo y métricas de evolución de la postura de seguridad.
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.	SI	La solución tecnológica TrendIA Vision One, proporciona una vista unificada del riesgo organizacional con métricas, tendencias, activos expuestos e indicadores que apoyan la toma de decisiones y el seguimiento de la postura de seguridad.
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.	SI	La solución tecnológica TrendIA Vision One, permite realizar análisis de riesgo sobre buzones de correo e identidades, detectando configuraciones inseguras, accesos sospechosos y anomalías de comportamiento de los usuarios.
13.6	La solución debe poder gestionar todos los activos descubiertos desde una única consola de gestión unificada.	SI	La solución tecnológica TrendIA Vision One, permite gestionar los activos descubiertos desde una consola unificada de administración y monitoreo.
13.7	La solución debe poder integrarse con proveedores externos para incorporar o enriquecer datos de la superficie de ataque.	SI	La solución tecnológica TrendIA Vision One, integra fuentes externas de datos que enriquecen la visibilidad y el análisis de la superficie de ataque desde una consola centralizada.
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).	SI	La solución tecnológica TrendIA Vision One, evalúa la postura de identidad mediante su integración con Active Directory, identificando configuraciones inseguras y generando indicadores de riesgo para los usuarios.
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,	SI	La solución tecnológica TrendIA Vision One, realiza barridos de IOC basados en inteligencia de amenazas del fabricante y

	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.		fuentes externas, permitiendo identificar amenazas presentes en el entorno y los activos afectados.
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.	SI	La solución tecnológica TrendIA Vision One, permite medir y comparar el nivel de riesgo de la organización mediante indicadores y métricas de referencia, facilitando la evaluación de su postura de seguridad.
13.11	La solución debe ser capaz de modificar la criticidad de un activo en función de la necesidad de la compañía.	SI	La solución tecnológica TrendIA Vision One, permite al administrador modificar la criticidad de los activos y ajustar su clasificación según las necesidades.
13.12	La solución debe tener soporte integrado para manuales de seguridad que puedan usarse para la remediación automatizada.	SI	La solución tecnológica TrendIA Vision One, dispone de Security Playbooks y Automation Center para soportar procesos de 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).	SI	La solución tecnológica TrendIA Vision One, permite identificar y evaluar de forma continua los activos expuestos a Internet mediante funcionalidades de gestión de 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.	SI	"La solución tecnológica TrendIA Vision One, genera una puntuación global de riesgo (Cyber Risk Index) basada en la evaluación continua de los riesgos.
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.	SI	La solución tecnológica TrendIA Vision One, calcula el riesgo de los activos considerando su criticidad, vulnerabilidades, actividad de amenazas y condiciones de seguridad del entorno.
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.	SI	La solución tecnológica TrendIA Vision One, genera un índice de exposición que mide continuamente la probabilidad de ocurrencia de amenazas y vulnerabilidades.
13.17	Debe utilizar múltiples proveedores de datos de descubrimiento (la dependencia del agente existente debe complementarse con proveedores de descubrimiento adicionales).	SI	La solución tecnológica TrendIA Vision One, integra múltiples fuentes de descubrimiento de activos, complementando la información obtenida por agentes con datos provenientes de otras tecnologías y sensores de seguridad.

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.	SI	La solución tecnológica TrendIA Vision One, proporciona métricas históricas de vulnerabilidades para activos internos y expuestos a Internet, incluyendo la identificación y seguimiento de CVE 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.	SI	La solución tecnológica TrendIA Vision One, proporciona métricas históricas de gestión de vulnerabilidades, incluyendo el tiempo promedio sin parches para activos internos y expuestos a Internet.
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.	SI	La solución tecnológica TrendIA Vision One, permite priorizar riesgos y recomendaciones de mitigación según los objetivos de reducción de riesgo.
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.	SI	La solución tecnológica TrendIA Vision One, cuenta con un panel ejecutivo que muestra la puntuación general de riesgo, el riesgo por activo, los ataques identificados y los principales factores de riesgo.
13.22	Los informes se pueden generar por demanda o mediante programación.	SI	La solución tecnológica TrendIA Vision One, permite generar reportes bajo demanda o de manera programada mediante plantillas predefinidas desde la consola de administración.
13.23	El contenido de los informes se puede filtrar para limitar la salida según criterios seleccionados	SI	La solución tecnológica TrendIA Vision One, permite filtrar y personalizar el contenido de los informes según criterios definidos por el administrador.
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).	SI	La solución tecnológica TrendIA Vision One, permite filtrar los activos por tipo, tecnología de descubrimiento, criticidad e índice de riesgo desde las vistas de inventario y operación.
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.	SI	La solución tecnológica Trend Vision One cumple con el requisito, al estar respaldada por reconocimientos de firmas globales de investigación tecnológica, destacándose su posicionamiento como Líder por Forrester en soluciones de gestión de superficie de ataque.
14.	**SOPORTE DEL FABRICANTE**		
14.1	El fabricante como mínimo debe: • Brindar soporte telefónico y basado en la web	SI	El contratista entregó las credenciales de acceso del portal de soporte y base de

	• 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.		conocimiento del fabricante a la supervisión del contrato, así como la matriz de soporte. Por otra parte, el contratista realizo la transferencia de conocimiento en la administración de la herramienta TrendAI Vision One, capacitación orientada a cinco (5) funcionaros de los grupos de GUTIC y CPD donde se abordaron temáticas de administración técnica/funcional y de configuración 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	SI	Con fecha 22/06/2026, se recibió mediante correo electrónico la matriz de escalamiento para el contrato 04-2-10024-2026, definiendo los cuatro niveles de escalamiento y tiempos de atención.
16.	**NIVEL DE EDUCACIÓN 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)	SI	El contratista entregó los documentos donde se evidenció objetivamente, que cumple los requisitos de formación y experiencia.

	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.	SI	El contratista entregó los documentos donde se evidenció objetivamente, que cumple los requisitos de formación y experiencia.
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 Externa Única de Colombia Compra Eficiente, Ítem 9.3 Acreditación de la formación académica.	SI	El contratista entregó los documentos donde se evidenció objetivamente, que cumple los requisitos de formación y experiencia.
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	SI	El contratista entregó mediante correo electrónico el 22/06/2026, el certificado donde se evidenció objetivamente, que es distribuidor autorizado del

			fabricante Trend Micro Colombia S.A.S.
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).	SI	El contratista entregó los documentos donde se evidenció objetivamente, que cumple los requisitos de formación y experiencia.
19.	**GARANTÍA TÉCNICA**		
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.	SI	El contratista mediante correo electrónico del 22/06/2026 entregó los documentos donde se evidenció objetivamente, que es distribuidor autorizado del fabricante y el certificado de autenticidad del licenciamiento.
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.	SI	La ejecución del contrato es hasta el 10/08/2026, así mismo el contratista realizó entrega de documento donde certifica atención por un periodo treinta y tres (33) meses siguientes a la finalización de la ejecución del contrato.
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.	SI	La ejecución del contrato es hasta el 10/08/2026, así mismo el contratista realizó entrega de documento donde certifica atención por un periodo treinta y tres (33) meses siguientes a la finalización de la ejecución del contrato.
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.	SI	El contratista realizo entrega de documento donde certifica atención del servicio por un periodo treinta y tres (33) meses siguientes a la finalización de la ejecución del contrato, indicando los tiempos de respuesta según lo descrito en el ítem.
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	SI	Las visitas de seguimiento, revisión, actualización y mejoras de la solución de seguridad Trend Vision One se agendarán de común acuerdo entre el

	de la herramienta tecnológica en DIPOL, garantizando al menos una (1) visita trimestral.		contratista y el administrador de la herramienta durante los treinta y tres (33) meses siguientes a la finalización de la ejecución del contrato. Así mismo, la empresa entregó un cronograma de visitas trimestrales de seguimiento de tipo orientativo para la ejecución de las mismas.

2.1. NOVEDADES, SITUACIONES ANORMALES O DE RELEVANCIA

Durante la ejecución del contrato no se presentaron situaciones anormales o de relevancia.

3. AVANCE DE LA EJECUCIÓN DEL CONTRATO U ORDEN DE COMPRA:

A la fecha de corte del presente informe de supervisión han transcurrido (78) días calendario desde que inició el plazo de ejecución del contrato u orden de compra, restando (0) días calendario para que finalice el pazo de ejecución.

Posterior al vencimiento del plazo de ejecución, transcurrieron (40) días calendario, correspondientes a la etapa de consolidación de entregables, revisión de informes finales y trámite administrativo.

4. TRÁMITES Y VERIFICACIÓN DE PAGOS:

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.

4.1. Ejecución Financiera y Pagos:

a. Balance general de pagos y entregas		
	Valor en pesos	**% del valor del contrato u orden de compra**
Valor total del contrato u orden de compra	$277.779.900,00	100%
Valor total de las entregas	$277.779.900,00	100%
Valor total facturado	$277.779.900,00	100%
Valor facturado pendiente de pago	$0	0%
Valor pagado	$277.779.900,00	100%
Valor pendiente de entrega	$0	0%

No. de acta o constancia de recibido	Valor recibido	Fecha de recibido	Valor facturado	No. factura	Valor pagado	Valor deducciones	No. orden de pago
01 del 15/07/2026	$277.779.900	25/05/2026 al 15/07/2026	$ 277.779.900	FE1135	$265.009.992	$12.789.908	291871926

4.2 Entrada de Bienes *(SI)*

Acta de recepción de bienes No. 005 del 07 de julio de 2026.

5. RECOMENDACIONES

El contratista ha cumplido sin ningún contratiempo con los compromisos y condiciones técnicas del contrato

6. CONCLUSIONES

El supervisor, deberá marcar con una (x) las casillas según corresponda al periodo entregado, con el fin de que la administración tenga claridad frente al cumplimiento o no del contratista. El no diligenciamiento será causal de la devolución del respectivo informe de supervisión.

El contratista cumplió con lo establecido en las cláusulas contractuales	**SI X**	Certifico con la firma del presente informe, que el contratista cumplió con las cláusulas y especificaciones técnicas del contrato, en la fecha o fechas establecidas, para lo cual relaciono y anexo los documentos soportes (técnicos obligatorios establecidos en las especificaciones técnicas, incluyendo las ambientales, de seguridad y salud en el trabajo y otros).
	NO___	En caso de incumplimiento parcial o total del contrato, se informó mediante comunicación oficial No. _____ del _____, dirigida al ordenador del gasto, las obligaciones incumplidas.

Atentamente,

Firma_____

Capitán YENNY MARCELA CORREDOR CRISTANCHO
Jefe Centro Protección de Datos
Supervisor Contrato No. 04-2-10024-2026
Correo electrónico: dipol.cpd-soc@dipol.gov.co
No. Celular: 3102184727