Corporación Autónoma Regional del Valle del Cauca

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

INFORME DE EVALUACIÓN TÉCNICA

SELECCIÓN ABREVIADA MENOR CUANTÍA No. 38 – 2021

Acorde con la designación como parte del Comité Evaluador de propuestas de la Selección Abreviada menor cuantía no. 38 – 2021, mediante memorando CVC No. 1103812021 del dieciséis (16) de diciembre de 2021, el Ingeniero Diego Alexander Millán Londoño, en su calidad de Jefe de la Oficina de Tecnologías de Información, se permite presentar la verificación de requisitos de carácter técnico habilitante y la evaluación y calificación de la propuesta presentada para participar en la Selección Abreviada menor cuantía no. 38 – 2021.

Las propuestas presentadas se evalúan con base en el documento de Pliego de Condiciones Definitivo de la Selección Abreviada menor cuantía no. 38 – 2021, consignado en el respectivo expediente del proceso de contratación.

1. OBJETO

Adquisición, implementación y soporte técnico de nivel 3 de licencias antivirus para la Corporación Autónoma Regional del Valle del Cauca.

2. PRELIMINARES

Firmas que presentaron propuesta:

- TECHNOLOGY PARTNERS.
- OPEN GROUP SAS.

Plazo de ejecución para el contrato:

El plazo para la ejecución del contrato se contará a partir de la firma de suscripción del acta de inicio, hasta el 31 de diciembre del 2021.

Disponibilidad Presupuestal:

Las obligaciones que se contraigan en desarrollo del presente proceso de contratación se atenderán con los recursos asignados para tal efecto del presupuesto de la Corporación para la vigencia 2021, el cual se estima en la suma de Ciento Sesenta y Un Millones Cuatrocientos Ochenta y Cinco Mil Ciento Cincuenta y Seis pesos Moneda Corriente ($161.485.156) incluido el impuesto del IVA%. Tal como se evidencia en el Certificado de Disponibilidad presupuestal No. 2832 de fecha 02 de diciembre de 2021 expedido por el Grupo de Presupuesto de la Corporación.

Corporación Autónoma Regional del Valle del Cauca

Comité Evaluador:

Mediante memorando CVC 1103812021 del dieciséis (16) de diciembre de 2021 y suscrito por el Director General de la CVC, se realizó el nombramiento del Comité Evaluador de propuestas para la Selección Abreviada menor cuantía no. 38 – 2021, así:

- Abog. Jairo España – Jefe Oficina Asesora Jurídica (C).
- Ing. Diego Alexander Millán Londoño - Jefe Oficina de Tecnologías de Información.
- Dra. Ingrid Ospina Realpe – Directora Financiera

Desde el ámbito de competencia de la Oficina de Tecnologías de Información, se realiza la respectiva verificación de los requisitos de carácter técnico habilitante (experiencia) y la respectiva evaluación de Calidad y Precio, de la propuesta recibida para la Selección Abreviada menor cuantía no. 38 – 2021.

VERIFICACIÓN TÉCNICA DE LA PROPUESTA:

Se realiza el presente estudio a la propuesta técnica y económica presentada de acuerdo al Pliego de Condiciones Definitivo, publicado el día nueve (09) de diciembre de 2021 el portal web del SECOP, en relación con la Selección Abreviada menor cuantía no. 38 – 2021.

3. ACEPTACIÓN DE LAS OBLIGACIONES DEL CONTRATISTA

Con base en lo requerido por la Corporación en el Numeral 2 OBLIGACIONES DEL CONTRATISTA del CAPITULO VI - ESPECIFICACIONES TÉCNICAS, del documento pliego definitivo de condiciones de la Selección Abreviada menor cuantía no. 38 – 2021, el proponente se compromete a cumplir de acuerdo en lo establecido según propuesta presentada.

REQUISITOS HABILITANTES

Experiencia del Proponente.

De acuerdo con lo establecido con el artículo 6 de la Ley 1150 de 2007 y en el Decreto 1082 de 2015, la experiencia se verificará con el RUP, el cual debe encontrarse actualizado y en firme. El Registro Único de Proponentes debe haber sido expedido por la Cámara de Comercio de su jurisdicción dentro de los treinta (30) días calendario anteriores a la fecha límite de recepción de propuestas del presente proceso de selección.

Proponentes nacionales o extranjeros con domicilio o sucursal en Colombia. Se requiere que el proponente acredite su experiencia con un (1) contrato, ejecutado y terminado a entera satisfacción en los últimos cinco (5) años, celebrado con entidades públicas o privadas, identificado con todos los códigos UNSPSC solicitados en la siguiente tabla, cuyo valor sea igual o superior al 100% del presupuesto oficial de este proceso, expresado en SMMLV, lo que se certificará con el RUP, actualizado y en firme.

La clasificación de Bienes y Servicios debe ser de acuerdo con la siguiente tabla:

Corporación Autónoma Regional del Valle del Cauca

UNSPC	NOMBRE
43222500	Equipo de seguridad de red
43233200	Software de seguridad y protección
43232700	Software de aplicaciones de red
81111800	Servicios de sistemas y administración de componentes de sistemas
81112200	Mantenimiento y soporte de software

Verificación

PROPONENTE	Codigo	NOMBRE	Folio soporte RUP	Cumple
TECHNOLOGY PARTNERS S.A.S.	43222500	Equipo de seguridad de red	5	SI
	43233200	Software de seguridad y protección	5	SI
	43232700	Software de aplicaciones de red	5	SI
	81111800	Servicios de sistemas y administración de componentes de sistemas	5	SI
	81112200	Mantenimiento y soporte de software	5	SI

PROPONENTE	Codigo	NOMBRE	Folio soporte RUP	Cumple
OPEN GROUP S.A.S.	43222500	Equipo de seguridad de red	8	SI
	43233200	Software de seguridad y protección	9	SI
	43232700	Software de aplicaciones de red	9	SI
	81111800	Servicios de sistemas y administración de componentes de sistemas	11	SI
	81112200	Mantenimiento y soporte de software	11	SI

Se requiere que el proponente acredite experiencia con un (1) contrato cuyo valor sea igual o superior al 100% en SMMLV del valor del presente proceso de selección.

Corporación Autónoma Regional del Valle del Cauca

Verificación:

TECHNOLOGY PARTNERS S.A.S., con RUP expedido de fecha DIC-15-2021.	43222500 43233200 43232700 81111800 81112200	Cto. No 8327, Conse. RUP No. 3, Folio 6.	1	177.74	885.87	**SI**

Observación: El contrato reportado por la empresa TECHNOLOGY PARTNERS S.A.S., cumple con los códigos UNSPSC solicitados, de igual forma cumple con los Valores establecidos para el pliego en SMMLV.

OPEN GROUP SAS., con RUP expedido de fecha Nov-19-2021.	43222500 43233200 81111800 81112200	Cto. CPS-PR2020-220, Conse. RUP No. 69, Folio 45.	1	177.74	1697,48	**NO**

Observación: El contrato reportado por la empresa OPEN GROUP SAS, no cumple con la totalidad de los códigos UNSPSC solicitados, el código 43232700 no se encuentra registrado en la clasificación de bienes, obras y servicios que en relación a los bienes, obras y servicios que ofrecerá a las entidades Estatales en el RUP, en el contrato presentado.

La empresa OPEN GROUP SAS, no presenta documentos para subsanación.

Se debe acreditar que el contrato que presenta tenga como objeto o alcance, la venta e implementación de una cantidad igual o mayor a 836 licencias antivirus., La acreditación debe realizarse mediante certificaciones; actas de recibo final a satisfacción o actas de liquidación, en las

cuales se pueda validar la información solicitada no contenida en el RUP; estos documentos deben contener como mínimo lo siguiente:

Haber sido suscritos por el representante legal de la entidad contratante o por el director del área técnica encargada o por el funcionario delegado para tal fin.

Nombre del Contratista,
Número y objeto del contrato,
Actividades ejecutadas,
Valor ejecutado,
Plazo de ejecución, fechas de iniciación y de terminación,
Porcentaje de participación si el contrato fue ejecutado en Consorcio o Unión Temporal.
Indicar que fue recibido a satisfacción.

La experiencia del oferente plural (unión temporal, consorcio o promesa de sociedad futura) corresponde a la suma de la experiencia que acredite cada uno de los integrantes de éste, afectada por el porcentaje de participación, cada integrante debe aportar a la experiencia solicitada.

Verificacion:

TECHNOLOGY PARTNERS S.A.S.,	1. Certificación expedida por BANACOL. Contrato No 8327, en cumplimiento del Objeto: El contratista se obliga a entregar el "Suministro Licencias solución integral de seguridad informática para tecnologías de Información que incluye protección interna, perimetral (correo, antispam, filtrado U´RLS, IPS) y en la nube, Instalación, configuración, capacitación, gestión, monitoreo y soporte. En total se suministraron 875 licencias", Evidencia FORMATO 3-EXPERIENCIA DEL PROPONENTE, folios 2.	SI	
OPEN GROUP SAS	Certificación expedida RED COLOMBIANA DE INSTITUCIONES DE EDUCACION SUPERIOR – EDURED. Contrato No CPS-PR2020 – 220, en cumplimiento del Objeto: El contratista se obliga a entregar el "soporte de fabricante y proveedor 7 *24 y licenciamiento de la plataforma de seguridad informática perimetral existente conformada por dos dispositivos Checkpoint 16000 (alta disponibilidad) y la generadora de reportes Smart console 625, por periodo de 12 meses. Contratar la adquisición, instalación, configuración y puesta en funcionamiento de una solución de control de acceso a redes NAC (Network Access Control) y Contratar la solución	SI	

	de seguridad de antivirus para 5500 equipos, que permita la actualización, integración y fortalecimiento de las herramientas de análisis de seguridad en computadores y servicios informáticos críticos para la Alcaldía de Santiago de Cali.", Evidencia, 69.Edured Certificacion.pdf.		

Certificaciones de Fabricante

Solo serán habilitados los oferentes que aporten certificación emitida por el fabricante, donde certifique estar registrado en su programa de canales/partners y donde certifique mínimo 5 años de estar dentro de los tres más altos niveles de canal/partner, y que cuenta con capacidad para: comercializar e implementar las soluciones de dicho fabricante en el territorio colombiano.

No se aceptarán certificaciones emitidas por mayoristas, distribuidores u otro tercero diferente al fabricante. Dichas certificaciones deberán contar con fecha de expedición no mayor a 60 días anteriores a la fecha de presentación de la oferta.

Verificación:

TECHNOLOGY PARTNERS S.A.S.,	Certificación expedida por TREND MICRO, con fecha 15 de Diciembre de 2021. Con más de 5 años de estar dentro de los tres más altos niveles de canal/partner.	SI
OPEN GROUP SAS	Certificación expedida por TREND MICRO, con fecha de Diciembre de 2021. Con **menos** de 5 años de estar dentro de los tres más altos niveles de canal/partner	No

La empresa OPEN GROUP SAS, no presenta documentos para subsanación.

Del Personal Requerido

Se requiere que el proponente certifique en la carta presentación de la Propuesta, la experiencia del equipo de trabajo según los perfiles profesionales de cada integrante, sus respectivos soportes y demás documentos legales que así lo acrediten dando cumplimiento a la siguiente información requerida por la Corporación:

Experiencia del Equipo de Trabajo:

El proponente deberá disponer del siguiente equipo de Trabajo y acreditar su experiencia, así:

Un (1) Gerente de Proyectos: Ingeniero Industrial, Electrónico, Sistemas o Telemático, para desarrollar la planeación y ejecución de las fases del proyecto:

- Experiencia general mínima de cinco (5) años contados a partir de la finalización de las materias
- Experiencia específica mínima de cinco (5) años ejerciendo cargos relacionados con funciones de gerencia o dirección en el sector de las TIC.

Un (1) Tecnólogo/Ingeniero Líder diseñador de políticas de seguridad informática: Tecnólogo/Ingeniero Industrial, Electrónico, Sistemas, Telemático o administración de redes con:

- Experiencia general mínima de cinco (5) años trabajando en empresas del sector TIC, contados a partir de la terminación de materias.
- Experiencia específica mínima de ocho (8) meses ejerciendo funciones como configurador, operador y/o administrador de tecnologías de infraestructura o software.
- Especialización en Seguridad Informática o en su defecto contar con todas las siguientes certificaciones: CISSP y CISM y CEH-Ethical Hacking, e ISO27001:2013, vigentes a la fecha de la presentación de la oferta.
- Certificado de fábrica en nivel fundamentos y/o profesional en plataformas de protección de Endpoint, protección de servidores y XDR, con una fecha de expedición no mayor a 2 años, de la misma marca ofertada para el presente proceso.

Un (1) Tecnólogo/Ingeniero de seguridad de endpoint y protección de información: Tecnólogo/Ingeniero Electrónico, Sistemas, Telemático o administración de redes, para la validación técnica, implementación y ajustes sobre las plataformas de seguridad de endpoint y protección de información DLP, con:

- Experiencia general mínima de tres (3) años trabajando en empresas del sector TIC, contados a partir de la terminación de materias.
- Experiencia específica mínima de dos (2) años como implementador, analista o administrador de soluciones de seguridad de endpoint y DLP.
- Certificado de fábrica en nivel fundamentos, esencial o profesional en plataformas de protección de Endpoint, protección de servidores o XDR, con una fecha de expedición no mayor a 2 años de la misma marca ofertada para el presente proceso.

Verificación:

TECHNOLOGY PARTNERS S.A.S.,	Ingeniero Industrial, Electrónico, Sistemas o Telemático – **Cumple**	**SI** Profesional propuesto con más de 5 años de experiencia profesional. Mas de 5 años ejerciendo cargos relacionados con funciones de gerencia o dirección en el sector de las

Corporación Autónoma Regional del Valle del Cauca

		TIC. se anexa certificación que acredita Experiencia, Evidencia Archivo Gerente de Proyectos.
OPEN GROUP SAS	Ingeniería Ingeniero Industrial, Electrónico, Sistemas o Telemático – **Cumple**	**SI** Profesional propuesto con más de 5 años de experiencia profesional, Mas de 5 años ejerciendo cargos relacionados con funciones de gerencia o dirección en el sector de las TIC. se anexa certificación que acredita Experiencia, Evidencia Archivo Gerente.pdf

TECHNOLOGY PARTNERS S.A.S.,	Tecnólogo/Ingeniero Industrial, Electrónico, Sistemas, Telemático o administración de redes – **Cumple** Especialización en Seguridad Informática o en su defecto contar con todas las siguientes certificaciones: CISSP y CISM y CEH-Ethical Hacking, e ISO27001:2013, vigentes a la fecha de la presentación de la oferta – **No cumple**	**NO** Tecnólogo propuesto con más de 5 años de experiencia. Mas de (8) meses de experiencia ejerciendo funciones como configurador, operador y/o administrador de tecnologías de infraestructura o software. No se evidencia acta o diploma de Especialización en Seguridad Informática. Por lo cual no cumple con el perfil requerido.

Corporación Autónoma Regional del Valle del Cauca

OPEN GROUP SAS	Tecnólogo/Ingeniero Industrial, Electrónico, Sistemas, Telemático o administración de redes – **Cumple** Especialización en Seguridad Informática o en su defecto contar con todas las siguientes certificaciones: CISSP y CISM y CEH-Ethical Hacking, e ISO27001:2013, vigentes a la fecha de la presentación de la oferta – **No cumple**	**SI** Profesional propuesto con más de 5 años de experiencia profesional. Mas de (8) meses de experiencia ejerciendo funciones como configurador, operador y/o administrador de tecnologías de infraestructura o software. Se evidencia diploma de Especialización en Seguridad Informática. Evidencia Archivo. LIDERSEG.pdf

En informe de evaluación de propuestas publicado el día 17/12/2021, se solicita subsanar novedades encontradas en la verificación de requisitos habilitantes para el Perfil: Tecnólogo/Ingeniero Líder diseñador de políticas de seguridad informática, por lo anterior la empresa TECHNOLOGY PARTNERS S.A.S., envía documento Subsanación Técnica CVC el día 21/12/2021 3:30 PM, donde presenta Tecnólogo con más de 5 años de experiencia, Mas de (8) meses de experiencia ejerciendo funciones como configurador, operador y/o administrador de tecnologías de infraestructura o software, y se evidencia diploma de Especialización en Seguridad Informática. Por lo cual cumple con el perfil requerido

TECHNOLOGY PARTNERS S.A.S.,	Tecnólogo/Ingeniero Electrónico, Sistemas, Telemático o administración de redes – **Cumple.**	**SI** Tecnólogo propuesto con más de 3 años de experiencia. Mas de (2) años como implementador, analista o administrador de soluciones de seguridad de endpoint y DLP. Evidencia Archivo. Ingeniero de Seguridad.pdf

OPEN GROUP SAS	Tecnólogo/Ingeniero Electrónico, Sistemas, Telemático o administración de redes – **Cumple.**	**SI** Profesional propuesto con más de 5 años de experiencia profesional. Mas de (2) años como implementador, analista o administrador de soluciones de seguridad de endpoint y DLP. Evidencia Archivo. INGENDPOINT.pdf

Se evidencia comprobantes de pago de aportes a seguridad social realizado por la empresa TECHNOLOGY PARTNERS S.A.S., de los meses de septiembre, octubre y noviembre de 2021.

Se evidencia comprobantes de pago de aportes a seguridad social realizado por la empresa OPEN GROUP SAS, de los meses de septiembre, octubre y noviembre de 2021, donde No se evidencia pago de aportes del personal propuesto para el perfil de Tecnólogo/Ingeniero Líder diseñador de políticas de seguridad informática.

La empresa OPEN GROUP SAS, no presenta documentos para subsanación.

4. EVALUACIÓN DE LAS PROPUESTAS Y SELECCIÓN DEL CONTRATISTA

Acorde con el resultado del numeral anterior, se continúa en la fase de evaluación con fundamento en los criterios de calidad, apoyo a la Industria Nacional y precio, según lo consignado en el *CAPITULO IV PROCESO DE PONDERACIÓN DE PROPUESTAS Y SELECCIÓN DEL CONTRATISTA* del Pliego de Condiciones Definitivo. Dado que existe un proponente habilitado para esta fase, se aplicarán los criterios de evaluación a la firma **TECHNOLOGY PARTNERS S.A.S.,** con el fin de asignar el puntaje que corresponda según su propuesta.

Ponderación para la modalidad del proceso de Licitación Pública: Para determinar la oferta más favorable la CVC tendrá en cuenta la ponderación de los elementos de calidad y precio, soportados en puntajes y/o formulas.

FACTOR	CRITERIOS DE PONDERACION	PUNTAJE
Económico	Precio (fórmula)	40 puntos
Técnico	Calidad (puntaje)	60 puntos
Total		**100 Puntos**

* Incentivos a la industria nacional y Proponentes con trabajadores discapacitados

Corporación Autónoma
Regional del Valle del Cauca

A. Factor Económico - Precio: Se asignará un puntaje máximo de 40, aplicando como método de cálculo del puntaje para el factor precio la Media Geométrica con Presupuesto Oficial, consiste en establecer la media geométrica de las Ofertas válidas y el presupuesto oficial un número determinado de veces y la asignación de puntos en función de la proximidad de las Ofertas a dicha media geométrica, como resultado de aplicar las fórmulas que se indican en seguida. Para el cálculo de la media geométrica con presupuesto oficial se tendrá en cuenta el número de Ofertas válidas y se incluirá el presupuesto oficial del Proceso de Contratación en el cálculo tantas veces como se indica en el siguiente cuadro:

Número de propuestas (n)	Número de veces en las que se incluye el presupuesto oficial (nv)
1 a 3	1
4 a 6	2
7 a 9	3
10 a 12	4
13 a 15	5
.....	.....

Y así sucesivamente por cada tres propuestas válidas se incluirá una vez el presupuesto oficial del proceso de contratación.

Seguidamente se determinará la media geométrica con la inclusión del presupuesto oficial de acuerdo a lo establecido en el cuadro anterior mediante la siguiente fórmula:

$$MGPO \quad \sqrt[(nv+n)]{PO * PO * \cdots POnv * P1 * P2 * \cdots Pn}$$

$$\sqrt[(nv+n)]{PO * PO * \cdots POnv * P1 * P2 * \cdots Pn}$$

Dónde:

MGPO = Media geométrica con presupuesto oficial.
N = Número de propuestas válidas.
nv = Número de veces que se incluye el presupuesto oficial (PO).
PO = Presupuesto oficial.
Pn = Valor de la propuesta económica corregida del proponente i.

Obtenida la media geométrica con presupuesto oficial se procederá a ponderar las propuestas de acuerdo con la siguiente formula.

$$\text{Puntaje i para valores menores o iguales a MGPO= 600} \times \left[1 - \left[\frac{MGPO - Vi}{MGPO}\right]\right]$$

$$\text{Puntaje i para valores mayores a MGPO= 600} \times \left[1 - 2\left[\frac{|MGPO - Vi|}{MGPO}\right]\right]$$

Donde
MGPO = Media geométrica con presupuesto oficial
Vi = Valor total corregido de cada una de las propuestas i
i = Número de propuesta

En el caso de propuestas económicas con valores mayores a la media geométrica con presupuesto oficial se tomará el valor absoluto de la diferencia entre la media geométrica con presupuesto oficial y el valor de la propuesta, como se observa en la fórmula de ponderación.

En todo caso, cuando el valor de la propuesta supere el presupuesto oficial establecido, aplicará causal de rechazo contenida en el pliego de condiciones.

B. Factor Calidad: Se asignará un puntaje máximo de 60 puntos al proponente que oferte: Una (1) Capacitación virtual para la mesa de ayuda de la corporación de ocho (8) horas, orientada a la implementación y soporte técnico de los clientes antivirus.

Lo cual se acreditará mediante una carta firmada por el representante legal del oferente, donde se compromete a dictar estrictamente la capacitación señalada.

Verificación

La empresa **TECHNOLOGY PARTNERS S.A.S.** certifica que brindara una (1) Capacitación virtual para la mesa de servicio integral de la corporación de ocho (8) horas, orientada a la implementación y soporte técnico de los clientes antivirus, evidenciado en FORMATO No 7. Por lo anterior se asignan 60 puntos.

C. Incentivos: Apoyo a la industria nacional. Los proponentes pueden obtener puntaje de apoyo a la industria nacional por: i) Servicios Nacionales o Bienes Colombianos o por Trato Nacional. ii) Por la Incorporación de Servicios Nacionales o Bienes Colombianos.

La CVC en ningún caso otorgará simultáneamente el puntaje por: i) Servicio Nacional o Bienes Colombianos o por Trato Nacional. ii) Incorporación de Servicios Nacionales o Bienes Colombianos.

Los puntajes para estimular la industria nacional se relacionan en la siguiente tabla:

Concepto	Puntos

Promoción de servicios nacionales o con trato nacional	10
Incorporación de componente nacional en servicios extranjeros	5

Para que el proponente obtenga puntos por servicios nacionales debe presentar: i) Persona natural colombiana, la cédula de ciudadanía del proponente. ii) Persona natural extranjera residente en Colombia, la visa de residencia que le permita la ejecución del objeto contractual de conformidad con la ley. iii) La persona jurídica constituida en Colombia, el certificado de existencia y representación legal emitido por las Cámara de Comercio.

Para que el proponente extranjero obtenga puntaje por trato nacional debe acreditar que los servicios son originados de los estados mencionados en la sesión de acuerdos comerciales aplicables al presente proceso de contratación, información que se acreditará con los documentos que aporte el proponente extranjero para acreditar su domicilio.

Verificación

La empresa **TECHNOLOGY PARTNERS S.A.S**, certifica que cumple con los requisitos solicitados para obtener puntos por servicios nacionales lo cual se evidencia en los documentos presentados, Cámara de comercio 26-11-2021, RUP, RUT y FORMATO 8 INDUSTRIA NACIONAL.pdf. Por lo anterior se otorgan **10 puntos** por Concepto de Promoción de servicios nacionales o con trato nacional.

Incorporación del componente nacional en servicios extranjeros: La entidad asignara el puntaje descrito en la siguiente tabla a los proponentes extranjeros sin derecho a trato nacional que incorporen el porcentaje de personal calificado colombiano como se describe a continuación.

Porcentaje de Personal	Puntos

Incentivo para proponentes con trabajadores con discapacidad. La CVC asignará el uno por ciento (1%) del total de los puntos establecidos en el pliego de condiciones, a los proponentes que acrediten la vinculación de trabajadores con discapacidad en su planta de personal, de acuerdo con los siguientes requisitos:

1. La persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda, certificará el número total de trabajadores vinculados a la planta de personal del proponente o sus integrantes a la fecha de cierre del proceso de selección.

2. Acreditar el número mínimo de personas con discapacidad en su planta de personal, de conformidad con lo señalado en el certificado expedido por el Ministerio de Trabajo, el cual deberá estar vigente a la fecha de cierre del proceso de selección.

Verificados los anteriores requisitos, se asignará el 1%, del total de los puntos establecidos en el pliego de condiciones, al proponente que quienes acredite el número mínimo de trabajadores con discapacidad, señalados a continuación:

Corporación Autónoma Regional del Valle del Cauca

Número total de trabajadores de la planta de personal del Proponente	Número Mínimo de Trabajadores con Discapacidad Exigido.
Entre 1 y 30	1
Entre 31 y 100	2
Entre 101 y 150	3
Entre 151 y 200	4
Más de 200	5

Si la oferta es presentada por un consorcio, unión temporal o promesa de sociedad futura, se tendrá en cuenta la planta de personal del integrante del proponente plural que aporte como mínimo el cuarenta por ciento (40%) de la experiencia requerida para la respectiva contratación.

VERIFICACION ANEXO TECNICO:

TECHNOLOGY PARTNERS S.A.S.

La Corporación busca adquirir e implementar la renovación de licencias de 836 licencias de solución de protección para endpoint con integración incluida a plataforma XDR y 166 licencias para asociar a la plataforma XDR los equipos de cómputo que actualmente cuentan con solución de protección de endpoint en la institución en la sede principal, en las sedes DAR y subsedes.

Para dar cumplimiento a los requerimientos técnicos de los equipos activos suministrados los proponentes deberán adjuntar las hojas de datos o datasheet de los respectivos fabricantes. Los manuales, vínculos a páginas web y fichas técnicas provistas por los fabricantes podrán ser entregadas en idioma inglés.

ITEM	LICENCIAMIENTO	ESPECIFICACIÓN	DESCRIPCIÓN	CUMPLE SI/NO	OBSERVACIONES
1	solución de protección para endpoint con integración incluida a plataforma XDR	MARCA	TREND MICRO		
1.1.1		VERSIÓN	Licencias software cloud para protección para endpoint TREND MICRO APEX ONE CLOUD + XDR		
1.1.2		CANTIDAD	836	SI	
1.1.3		SOLUCIÓN DE PROTECCIÓN PARA ENDPOINT	Debe ser una solución que fusione una serie de técnicas avanzadas de protección contra amenazas entregadas a través de una arquitectura de agente único	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2

1.1.4			La solución debe tener la capacidad de brindar proteccion con los siguientes elementos: machine learning de alta fidelidad (en pre-ejecución y en ejecución), análisis de comportamiento (contra ataques de scripts, inyección, ransomware, memoria y navegadores), análisis en memoria para identificación de malware fileless, protección contra variantes, reputación web, prevenció de explotación de vulnerabilidades, bloque de comando y control, protección contra fuga de información DLP, control de dispositivos y aplicaciones, recuperación ante ransomware (ransomware rollback), detección y respuesta extendida XDR	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2
1.1.5			Debe contar con los siguientes módulos de protección incluídos dentro del licenciamiento sin la necesidad de activar a adquirir licenciamientos adicionales: Antimalware, Reputación Web, Firewall, Machine Learning, IDS/IPS, Control de aplicaciones, Data Loss Prevention DLP, Control de dispositivos.	SI	"https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000008um1zQAA Trend Micro SOLUTION OVERVIEW poster"
1.1.6			La solución debe brindar alta disponibilidad del servicio	SI	https://success.trendmicro.com/solution/1119782-servicelevel-objectives-oftrend-micro-apexone-as-a-service
1.2.1		CONSOLA DE ADMINISTRACION	La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.	SI	www.trendmicro.com/en_us/business/technologies/contr olmanager.html?modal=s3a-icondatasheet-956398 Apex central
1.2.2			La consola de administración debe estar despleagada en la Nube para garantizar la administración en todo el tiempo sin importar el lugar donde estén las maquinas administradas	SI	"www.trendmicro.com/en_us/business/technologies/contr olmanager.html?modal=s3a-icondatasheet-956398 Apex central Datasheet"

1.2.3			La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-onepatch-4-onlinehelp/introductionand-get/gettingstartedwith_002/product_short_named_001/client_computer_sing_002.aspx
1.2.4			La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.	SI	"https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/queryinglogs.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/notifications_001/event-notifications.aspx"
1.2.5			La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.	SI	www.trendmicro.com/en_us/business/technologies/controlmanager.html?modal=s3a-icondatasheet-956398 Apex central Datasheet"
1.2.6			La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/queryinglogs/log-querydata-views.aspx
1.2.7			La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispyware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/queryinglogs/log-querydata-views.aspx

1.2.8			La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/queryinglogs/log-querydata-views.aspx
1.2.9			La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/queryinglogs/log-querydata-views.aspx
1.2.10			La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/queryinglogs/log-querydata-views.aspx
1.2.11			La consola de administración debe tener la capacidad de generar reporte en formato PDF, DOCX y XLSX	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/reports_001/one-timereports/generatingone-time-.aspx
1.2.12			La consola debe poder operarse en la nube sin requerir recursos de infraestructura y entregarse como software como servicio	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet

1.2.13			La solución debe tener la capacidad de finalizar sesiones en la consola de administración por tiempo de inactividad	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/gettingstarted/the-webconsole/configuring-web-cons.aspx
1.2.14			La solución debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes, para que estos sean eliminados con una frecuencia especifica	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/productintegration/managed-productregi_001/managedservers/configuringproxyse.aspx#GUID-8D766EB4-FB16-4B61-9619-CE843B69C82B
1.2.15			La solucion debe permitir la configuracion de proxy tanto para los agentes como para el servidor de administracion.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/productintegration/managed-productregi_001/managedservers/configuringproxyse.aspx#GUID-8D766EB4-FB16-4B61-9619-CE843B69C82B
1.2.16			La solución debe permitir la realización de backups de los datos de configuraciones de la solución, los certificados SSL, datos de los agentes, y logs almacenados en el servidor de administración.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/policies/policymanagement_001/policymanagement_002/importing-andexport.aspx
1.2.17			La solución debe permitir la realización de backups de los logs almacenados en los agentes.	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/updates-andadminist/administration_001/generaladministrati/migrati

					ng-from-anon/ using-theserver-mig/theservermigration.aspx
1.2.18			La consola de administración de la solución debe proporcionar gráficos y estadísticas de distribución de la solución, distribución de políticas y agentes administrados.	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/dashboard/summary-tab.aspx https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/dashboard/operation-centertab.aspx https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/dashboard/compliance-tab.aspx
1.2.19			La solución debe tener la capacidad de identificar o agrupar los logs por políticas, inventario de equipos, aplicaciones conocidas, acciones del administrador, mensajes de los agentes y mensajes del servidor.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/configuringlog-aggr.aspx
1.2.20			La solución debe permitir realizar una sincronización de la lista de objetos sospechosos obtenidos de otras soluciones del mismo fabricante.	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/threatdefense/connectedthreatdef_001/suspicious

					-objectli/ suspicious-objectli_ 001.aspx
1.2.2 1			La solución debe contar con roles definidos con diferentes niveles de acceso para editar y/o visualizar los datos y configuraciones de la solución.	SI	https://docs.trendmicro.com/enus/ enterprise/trendmicro-apex-central-2019-onlinehelp/ gettingstarted/ accountmanagement_ 001/ user-roles.aspx
1.2.2 2			La solución debe permitir realizar búsquedas en los registros o logs, haciendo uso de filtros y permitir exportarlos en archivos con formato (CVS o XLSX).	SI	https://docs.trendmicro.com/enus/ enterprise/apexcentral-as-aservice-onlinehelp/ detections/logs _001/queryinglogs. aspx
1.2.2 3			Se podrán crear usuario y roles para el acceso a la plataforma de administración	SI	https://docs.trendmicro.com/enus/ enterprise/trendmicro-apex-central-2019-onlinehelp/ gettingstarted/ accountmanagement_ 001/ user-roles.aspx

1.2.24			La solución propuesta debe contar con un Dashboard el cual permita visualizar en tiempo real C&C, Ancho de banda usado, amenazas detectas, estado del servidor, estado de los agentes	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/dashboard/summary-tab.aspx https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/dashboard/operation-centertab.aspx https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/dashboard/compliance-tab.aspx https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/dashboard/threat-detectiontab.aspx
1.2.25			Es requisito contar con la habilidad de configurar permisos granulares en la consola de administración para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos, pero sin la capacidad de modificar ninguna configuración	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/gettingstarted/accountmanagement/userroles-saas-/editinga-user-role.aspx
1.3.1		AGENTES	Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/productintegration/securityagentinsta_001/downloading-security.aspx

1.3.2			Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-onepatch-4-onlinehelp/protectingtrend_cli/installingthetrend/trend_client_program_007/thetrend_client_pro/uninstall_program_gr.aspx
1.3.3			Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/policies/policymanagement_001/policymanagement_002/creating-a-newpolic/specifyingpolicyta.aspx#GUIDD0127C9A-A7FB-49C8-AF9C-9DD5AA3FF4C6
1.3.4			El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE
1.3.5			El agente debe estar integrada en un solo agente para dar protección de amenazas, protección de vulnerabilidades, control de aplicaciones y DLP	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE
1.3.6			Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc), si alguna de estas es inaccesible para el agente.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-onepatch-4-onlinehelp/protectingtrend_cli/keepingprotectionu_001/updateCra.

					info@techno-partners.com - www.techno-partners.com agents/updatesources-foru/ standard-updatesour. aspx
1.3.7			Los agentes de proteccion de los equipos deben tener la capacidad de protegerse contra intentos de desinstalacion o cancelacion de los procesos por los usuarios o por una aplicación de terceros.	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentpro_001/coexistand-fully-fe.aspx
1.3.8			La solución debe permitir el uso de protocolos SSL para la comunicación entre los agentes y el servidor de administración.	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/introduction/introducing-control-/key-features-andben. aspx
1.4.1		/ Regulatorios y cumplimiento	La solución debe estar ubicada en el cuadrante de líderes de Gartner conocido como "Magic Quadrant for Endpoint Protection Platforms" mínimo en los últimos 5 años anteriores.	SI	https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html?_ga=2.22624188.6690135.1615049478-670520027.1607008088
1.4.2			La solución debe estar listada como líder en el último cuadrante de Forrester de Endpoint Security Suites y Endpoint Detections and Responses	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.5.1		Sistemas Operativos soportados	Windows 7 (32-bit / 64-bit) Service Pack 1	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-. aspx

1.5.2			Windows 8.1 (32-bit / 64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-.aspx
1.5.3			Windows 10 (32-bit / 64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-.aspx
1.5.4			Windows Server 2008 R2 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx
1.5.5			Windows MultiPoint Server 2010 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx
1.5.6			Windows MultiPoint Server 2011 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx
1.5.7			Windows Server 2012 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx
1.5.8			Windows Server 2016 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/

					officescanagentdep/ officescanagentins/ officescanagent-sys/freshInstallations-_001.aspx
1.5.9			Windows Server 2019 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx
1.6.1		ANTIMALWARE	La solucion debe tener la capacidad de brindar proteccion contra malware, virus de red, conecciones sospechosas, amenazas web, spyware, trojanos, monitoreo de comportamiento, ataques conbinados y ataques de dia cero para equipos de punto final (Endpoint).	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagent-sca/antimalwarescannin_001/scanactions-=-osce-/activeaction.aspx
1.6.2			La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web.	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagent-sca/usingtheofficescan/officescan-firewall.aspx
1.6.3			La solución debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-onepatch-4-onlinehelp/protectingtrend_cli/scanningforsecurit_001/scantypes.aspx
1.6.4			La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación de este dentro de la red.	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagent-sca/antimalwarescannin_001/scanactions-=-osce-/custom-scanactions-/scan_set_cmn_act_qua.aspx

1.6.5			La solución debe permitir la integración con Active Directory	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/gettingstarted/activedirectoryand_001/activedirectory-int.aspx
1.6.6			La solución debe permitir realizar una migración a versiones superiores de la misma conservando las configuraciones, incluida la base de datos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/tools-andadditional/administering-theda/backing-updb_contro.aspx
1.6.7			La solución debe permitir recuperar los archivos que sean enviados a cuarentena.	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagent-sca/antimalwarescanning-001/restoring-quarantine.aspx
1.6.8			La solución debe proporcionar protección a los agentes contra Ramsomware	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.6.9			La solución debe proporcionar una consola de administración que pueda ser utilizada desde un entorno web.	SI	www.trendmicro.com/en_us/business/technologies/control-manager.html?modal=s3a-icondatasheet-956398 Apex central Datasheet
1.6.10			La solución debe tener la capacidad de analizar la reputación de archivos	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet

1.6.11			La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de la misma.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/gettingstarted/accountmanagement_001/user-roles.aspx
1.6.12			La solución debe tener la capacidad de proteger los equipos que se encuentren dentro de la red y fuera de ella	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentCra. 55 No. 40A - 20, Of. 506, PBX. (57)(4) 261 23 93, Fax. Ext. 22, Medellin, Colombia info@techno-partners.com - www.techno-partners.com pro_001/endpointlocation-sa.aspx
1.6.13			La solución debe tener la capacidad de programar las sincronizaciones de los equipos para horas y fechas específicas	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/productintegration/compon entupdates/configuring-schedule.aspx
1.6.14			La solución debe permitir la configuración de un servidor SMTP para el envío de notificaciones vía Email	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-one-2019-server-onlinehelp/managing-theproduct/managingtheproduct_001/administrator-notifi.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-one-2019-server-onlinehelp/managing-theproduct/managingtheproduct_001/administratornotifi/configuringgeneral-.aspx

1.6.15			La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando una amenaza sea detectada	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/notifications_001/contact-groups/addingcontact-group.aspx
1.6.16			La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/notifications_001/advanced-threatacti/email messages-with-.aspx
1.6.17			La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando uno de los equipos sea enviado a cuarentena.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/appendices/data-views_001/dataview_-security-/content-violationin/email-messageswith-_001.aspx
1.6.18			La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones cuando los equipos sean enviados a cuarentena.	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/detections/notifications/advancedthreat-acti/attackdiscovery-det.aspx
1.6.19			La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/monitoringofficesca/notifications_001/officescanagentnot/configuringvirus_ma.aspx
1.6.20			Protección de Exploración de la memoria: identificando procesos en ejecución a medida que se ejecuta en la memoria para determinar si es malicioso. Permite terminar el proceso en ejecución dependiendo de la configuración de la acción.	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO

					APEX ONE datasheet
1.6.21			Protección contra ataques de exploits: controla los programas que demuestran un comportamiento anormal asociado con ataques de exploits.	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.6.22			Protección de exploits de documentos: escanee documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.6.23			Aprendizaje automático: analiza archivos desconocidos de baja prevalencia al extraer características de los archivos para examinarlos utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso (es decir, malware / ransomware / amenazas de día 0).	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.6.24			Protección contra ransomware: busca la ofuscación / cifrado rápido de archivos mediante un proceso desconocido, elimina ese proceso y restaura los archivos cifrados.	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.6.25			La solucion debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tenre la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet

1.6.26			La solucion debe permitir proteger los equipos frente a vulnerabilidades no conocidas presentes en los equipos	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.7.1		DLP- DATA LOSS PREVENTION	La solucion debe tener la capacidad de prevenir y/o informar sobre la fuga o perdida de informacion sensible de la organización ya sea de forma accidental o deliberada.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_dlp.html#id125O40I20HS
1.7.2			La solucion debe permitir identificar o configurar los activos digitales que se desean proteger.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_dlp.html#id125O40I20HS
1.7.3			La solucion debe permitir la creacion de politicas que limiten la trasmision o transferencias de activos digitales por los canales de comunicación convencionales (email y/o dispositivos externos).	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_dlp.html#id125O http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_dlp.html#id125O40I20HS 40I20HS
1.7.4			La solucion debe tener la capacidad de igualmente brindar proteccion y aplicar politicas para transferencia de activos digitales mediante cliente de correo ya sera software o web.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_dlp.html#id125O40I20HS
1.7.5			La solucion debe permitir que la organización haga cumplir con las normas de privacidad establecidas.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_dlp.html#id125O40I20HS
1.7.6			La solucion debe tener la capacidad de brindar proteccion contra filtrado de datos sensibles y proporcionar un control de dispositivos, permitiendo confugurar reglas o politicas para ser aplicadas a grupos o agentes individuales.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_dlp.html#id125O40I20HS
1.7.7			La solucion debe proporcionar identificadores de datos y/o plantillas para la creacion de politicas.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_pol.html#id124RD

					J00W5Z
1.7.8			La solucion debe tener la capacidad de identificar o reconocer archivos ejecutables, documentos, graficos vectoriales, archivos multimedia, archivos comprimidos, bases de datos, hojas de calculo, presentacion, archivos vinculados e incrustados, y/o archivos encriptados.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_end_fea.html#id124NA0B0DYK
1.7.9			La solucion debe tener la capacidad de localizar activos digitales almacenados en portatiles, equipos de escriotorio, y servidores.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_end_fea.html#id124NA0B0DYK
1.7.10			La solucion debe tener la capacidad de proporcionar filtros de proteccion para canales de red como FTP o HTTP, canales de aplicaciones o perifericos.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_end_fea.html#id124NA0B0DYK
1.7.11			La solucion debe tener la capacidad de detectar datos estructurados y no estructurados.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_end_fea.html#id124NA0B0DYK
1.7.12			La solucion debe mantener un monitoreo constante.	SI	http://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_end_fea.html#id124NA0B0DYK
1.7.13			La solución debe proveer plantillas que permitan el cumplimiento de estándares como GLBA, HIPAA, PCI-DSS o SB-1386	SI	www.trendmicro.com/es_es/business/products/userprotection/sps/endpoint/integrateddata-lossprevention.html?modal=9dae4a
1.7.14			La solucion debe permitir generar un control de dispocitivos externos al equipo, generando bloqueos y alertas pero permitir dispocitivos por su ID,	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/introducingofficesc/introducing officesc_001/features-and-benefit.aspx
1.7.15			La solución debe permitir la integración con Directorio Activo y permitir la delegación de administración	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/adm_ldap-cfg.html

1.7.16			La solución debe contar con una consola de administración WEB que permita la configuración de políticas e implementaciones, reportes de los equipos, extracción de huellas digitales, y actualizaciones.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/gettingstarted/dashboard/data-lossprevention_001.aspx
1.7.17			La solucion debe tener la capacidad de identificar los activos digitales almacenados en los dispositivos o el trafico en la red utilizando expresiones regulares (predefinidas y/o personalizadas), atributos de archivos (tipo y/o tamaño), huellas digitales, palabras clave, y/o plantillas (predefinidas y/ personalizadas)	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/policies/policyresources_001/data-lossprevention_002/data-identifiertype.aspx
1.7.18			Las plantillas de identificación de activos digitales deben permitir combinar identificadores de datos (expresiones, atributos de archivos, huellas digitales, lista de palabras).	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_dat-id.html
1.7.19			La solución debe permitir usar plantillas predefinidas por el fabricante, personalizarlas, crear plantillas, importar plantillas, exportar plantillas, y eliminar las plantillas.	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_tmp.html
1.7.20			La solución debe permitir implementar políticas independientes tanto para agentes en los dispositivos como para agentes en la red.	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_pol.html
1.7.21			La solución debe permitir generar reportes ya sea por demanda o de forma programada (Diario, semanal o mensual), estos reportes deben contener información de los logs de los agentes. Dichos reportes deben mostrar información relevante como top de incidentes, información resumida, reporte de auditoria, entre otros.	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/rep_gen_new.html#id124NBJ002BL
1.7.22			La solución debe permitir almacenar reportes y estos deben estar disponibles en formatos PDF, HTML, o Microsoft Excel	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/rep_arc.html

1.7.23			La solución debe tener la capacidad de administrar los logs de manera que pueda eliminar los Logs que tengan un tiempo de más de 90 días, igualmente debe permitir la realización de un backup y limpieza de los mismos de forma manual.	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/log_cln_task.html#id124NE0TM04E
1.7.24			La solución debe soportar la detección de fuga de información en los siguientes tipos de archivo: .pdf .odt, .ott, .stw, .sxw .wpd, .wps .xml .xbd, .xdw .htm .jtd .sam .doc, .docm, .docx, .dot, .dotm, .dotx .wri .rtf .sgml .wsd, .bmp .dib .dcm .eps .img .gif .jpg .mac .png .tif, .tiff .ico .pcx, .dxf .dwg, .dws .cel, .dgn .cdb .CATDrawing, .CATPart, .CATProduct .cdr .dvi .gds .attr, .sgfx, .ssht .drw .ps .prt .svf .prtdot, .sldasm, .slddrw, .sldprt, .swf .aiff .mod .mov .avi .mid .mpeg .mpg .au .wav .wma .wmv, .7z .arc .arj .bz2 .Z .cpio .gz .lzh .chm .msg .pst .dbx .eml .pgp .rar .shar .tar .rpm .uue .zip, .sas .db .dif .dbf .fp7 .tbl .accdb, .mdb, ods, .ots, .stc, .sxc .csv .123 .wk1 .wk3 .wk4 .wke .wks .xlam .xlc .xls .xlsb .xlsm .xlsx .xltm .xltx .xlw .qpw .wb3 .wb2 .wb1 .wq1, .odp, .otp, .sti, .sxi .shw .pre .pot, .potm, .potx, .pps, .ppsm, .ppsx .ppt .pptm .pptx .vdw, .vdx, .vsd, .vss, .vst, .vsx, .vtx, .7z, .rar, .zip .accdb, .doc, .docx, .pdf, .ppt, .pptx, .wb1, .wb2, .wq1, .wpd, .xls, .xlsx, .mml .pub .qxp .one .mpp .hlp .iam, .idw, .ipt, .msoffice, .pqw y .plf	SI	https://docs.trendmicro.com/all/ent/dpref/v7.0/enus/dp_7.0_lists.pdf
1.7.25			La solución debe permitir configurar las fuentes de actualización para los parches o hot fixes y adicionalmente permitir configurar la periodicidad de las mismas.	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/upd_prd-evt_tsk.html
1.7.26			La herramienta de análisis local debe tener la capacidad de adquirir huellas digitales para los archivos almacenados en el equipo.	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_dat-id_fpt.html
1.7.27			La solución provee expresiones predefinidas para los números de tarjetas de crédito. A estos números se les realiza una verificación adicional por el número de prefijo y verificación con LUHN.	SI	https://docs.trendmicro.com/all/ent/dpref/v7.0/enus/dp_7.0_lists.pdf
1.7.28			La solución provee expresiones predefinidas para las direcciones de correo electrónico	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_datid_

					exp_cri.html
1.7.29			La solución provee expresiones predefinidas para los números de cuentas de bancos internacionales (IBAN).	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_datid_exp_cri.html
1.7.30			La solución provee expresiones predefinidas para códigos de identificación de negocio SWIFT BIC.	SI	https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/dat_datid_exp_cri.html
1.7.31			La solución provee una lista de palabras predefinidas para la validación de formularios como fecha de nacimiento, fecha de expiración, Nombres y apellidos, lugar de nacimiento, departamentos o ciudades y direcciones de domicilios.	SI	https://docs.trendmicro.com/all/ent/dpref/v7.0/enus/dp_7.0_lists.pdf
1.7.32			La solución provee una lista de palabras que pueden ser usadas en contextos ofensivos, racistas o que incluyan elementos para causar daño (armas)	SI	https://docs.trendmicro.com/all/ent/dpref/v7.0/enus/dp_7.0_lists.pdf
1.7.33			La solución provee una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.	SI	https://docs.trendmicro.com/all/ent/dpref/v7.0/enus/dp_7.0_lists.pdf
1.7.34			La solución debe permitir exportar e importar datos como políticas de seguridad y roles de usuarios	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/policies/policymanagement_001/policymanagement_002/importing-andexport.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/gettingstarted/user_endpoint-direct_001/userdetails.aspx

1.7.35			La solución debe permitir configurar y programar el reinicio de los dispositivos de forma que no afecte negativamente las operaciones de la organización.	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/productintegration/componentupdates/componentupdates_001/deployment-plan.aspx
1.7.36			la solución debe permitir la implementación de políticas para evitar que los usuarios publiquen contenido en clientes de mensajería instantánea o sitios de webmail	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/appendices/syslog-mappingcef/cef-dlp-logs/cefchannel-mapping-.aspx https://docs.trendmicro.com/all/ent/dlp/v5.6/enus/dlpe_5.6_olh/int_net_fea.html
1.8.1		CONTROL DE APLICACIONES	La solución debe tener la capacidad de prevenir la ejecución de aplicaciones no deseadas o desconocidas en los endpoint	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/policies/policyresources_001/application-control-/creatingapplication_001.aspx
1.8.2			La solución debe tener la capacidad de configurar acciones sobre los archivos que estén en la lista de Suspicious Objects proporcionada por el fabricante para sus soluciones de seguridad.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/threatdefense/connectedthreatdef_001/suspicious-object-li.aspx
1.8.3			La solución debe permitir bloquear o permitir aplicaciones de acuerdo a puntaje de seguridad propio del fabricante.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/policies/policyresources_001/application-control-/matchmethods/certifiedsafe-softw.aspx

1.8.4			La solución debe tener la capacidad de bloquear o permitir aplicaciones basada en patrones y puntaje de prevalencia de la aplicación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/policies/policyresources_001/application-control-/match methods/certifiedsafe-softw.aspx
1.8.5			La solución debe permitir establecer reglas para el cumplimiento de control de aplicaciones, dichas reglas deben permitir o bloquear aplicaciones de acuerdo con las políticas de la organización.	SI	https://docs.trendmicro.com/enus/enterprise/apexcentral-as-aservice-onlinehelp/policies/policyresources_001/application-control-.aspx
1.9.1		PROTECCION WEB	La solución debe contar con reputación web adicional reputación de archivos	SI	https://communitytrendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0694P000007tDIQQA2 TREND MICRO APEX ONE datasheet
1.9.2			La solución debe permitir el filtrado URL	SI	
1.9.3			La solución debe permitir realizar un control de Ancho de Banda	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/productintegration/managed-productregi_001/managedproductcomm/configuringmanaged-.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-apex-central-2019-onlinehelp/detections/logs_001/configuringlog-aggr.aspx

1.9.4			La solución debe permitir la inspección de trafico HTTP Y HTTPS	SI	https://success.trendmicro.com/solution/1122596-configuring-webreputation-servicesettings-in-apexone
1.9.5			La solución debe proteger la navegación en los equipos portátiles, endpoint y equipos que salen de la red corporativa	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentpro_001/endpointlocation-sa.aspx
1.9.6			El filtrado de URL de la solución debe estar definido por niveles de riesgo establecidos por el fabricante	SI	https://docs.trendmicro.com/all/ent/apex-svc/all/enus/apexCen_saas_ag.pdf
1.9.7			Si una URL no está en la base de datos para verificar su confiabilidad esta debe ser testada en tiempo real utilizando tecnología de categorización dinámica	SI	https://docs.trendmicro.com/all/ent/apex-svc/all/enus/apexCen_saas_ag.pdf
1.10.1		PLATAFORMA XDR	Debe permitir a la entidad tener la capacidad de detección y respuesta en email, endpoints, servidores, workloads en la nube y la red a través de una sola plataforma, es decir, poder hacer estas tareas de detección y respuesta en múltiples capas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.2			Debe proveer un mejor contexto y un análisis más profundo, para que la entidad pueda responder de forma más rápida y eficiente a amenazas, minimizando el impacto y alcance de un incidente en la organización	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.3			debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
1.10.4			Los modelos de correlación deben combinar multiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/features

1.10.5			La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
1.10.6			Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench.aspx
1.10.7			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	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-_benefit.aspx
1.10.8			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	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/workbenchdata.aspx
1.10.9			Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-.aspx
1.10.10			debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performing an-alert-/alertdetails.aspx
1.10.11			Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las acciones que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/

					analysischain.aspx
1.10.12			Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalytics-re.aspx
1.10.13			Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx
1.10.14			Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/search-syntaxsimple.aspx
1.10.15			Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain.aspx
1.10.16			Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/savedqueries.aspx
1.10.17			Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence-

					/intelligencereports/curatedintelligence.aspx
1.10.18			La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana 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	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/observedattack-tech.aspx
1.10.19			Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.20			En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.21			Debe ofrecer opciones de respuesta "context aware" para acciones rápida desde la plataforma.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.22			Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.23			Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx

1.10.24			Debe proveer un conector para Splunk nativo	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.25			Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.26			debe analizar la data recolectada por los sensoress para proveer alertas inteligentes, y detecciones de alta fidelidad.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/securityposturegro/identity-andrisk-in/riskinsights/cloud-apprisk-index/xdrdetections.aspx
1.10.27			Los sensores deben soportar integración nativa del vendor para obtener toda la data de actividad (telemetria, metadata, netflow) no solo data de alertas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.28			Los sensores deben soportar trabajar al menos en los siguientes sistemas operativos de Estaciones de trabajo de usuarios: Windows 7 y superior Mac OS X El Capitan 10.11 y superior	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/inventorymanagement_001/endpoint-inventory-2/xdr-sensorsupported.aspx

1.10.29			Los sensores deben soportar trabajar al menos en las siguientes sistemas operativos de servidores Windows (Windows 2008 y superior) Linux (Including visibility over docker containers attacks) Red Hat Enterprise Linux 6 y superior Ubuntu 16 y superior CentOS 6 y superior Debian 8 y superior Amazon Linux/Amazon Linux 2 Oracle Linux 6 y superior SUSE Linux Enterprise Server 12 y superior CloudLinux 7 y superior	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/inventorymanagement_001/endpoint-inventory-2/xdr-sensorsupported.aspx
1.10.30			Los sensores deben soportar trabajar por integración directa vía API con los proveedores de correo Microsoft 365 & G Suite	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/inventorymanagement_001/endpoint-inventory-2/xdr-sensorsupported.aspx
1.10.31			Los sensores deben soportar trabajar Network por integración nativa con sistema BDS	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdr-abou_001.aspx
1.10.32			En el caso de estaciones de trabajo de usuarios y servidores, la funcionalidad XDR debe ser una capacidad que puede tener embebida en el mismo agente de protección de endpoint. XDR no debe ser un agente adicional	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.33			Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
1.10.34			El vendor debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos to improve.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-

					benefit.aspx
1.10.35			Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/incident-view.aspx
1.10.36			El aplicativo de Detection Model Management debe permitir controlar el tipo de alertas que se disparan y se envían a Workbench.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
1.10.37			Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE. Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
1.10.38			Los modelos deben especificar para que productor en específico (Workstation/Server/Email/Network) aplica una alerta	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
1.10.39			Los modelos deben especificar y permitir modificar "status": encendido/apagado	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx

1.10.40			Los modelos deben especificar la ultima vez que se actualizó	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
1.10.41			Debe hacer una sección de excepciones dentro de la App de Model Management que despliegue todas las excepciones que se añadieron.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
1.10.42			La excepcion debe ser granular y debe mostrar lo siguiente: Object: El objeto que se ha añadido como excepción en una investigación Filter: El filtro que identificó el objeto como un indicador de amenaza Type: El atributo del objeto añadido Data field: Log definido por el objeto Match type: Exacto o Parcial (soporta wildcards) Description: Información definida por el usuario para la excepción Created: Fecha y hora en que se añadió la excepción Created by: Usuario que creó la excepción	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
1.10.43			Debe permitir añadir excepciones durante la investigación de una alerta.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
1.10.44			En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
1.10.45			Debe integrar inteligencia al minuto con reportes del vendor y terceras partes confiables para ayudar a identificar amenazas	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence-/intelligencereports/curatedintelligence.

					aspx
1.10.46			Debe poder analizar los logs, comparar la data contra los reportes de Threat Intelligence automáticamente, y generar alertas basadas en indicadores sospechosos o maliciosos detectados	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence-/intelligencereports.aspx
1.10.47			La App de Workbench debe mostrar alertas por los modelos de detección y permitir investigar a más detalle. La data del Workbench debe incluir: Status: New/In Progress/Closed/Closed – False Positive Score: basado en la severidad del modelo de detección y el impacto de la alerta. Workbench ID: identificador único para la alerta Model: Modelo que disparó la alerta Model severity: Severidad asignada al modelo que disparó la alerta Impact scope: Número de entidades afectadas por Servers/Workstations/Users/Cuentas de correo Created: Fecha y Hora que XDR generó la alerta	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/workbenchdata.aspx
1.10.48			Endpoint Profile: Debe incluir Hostname/IPv4/GUID/MAC Address/OS version/Producto/Último usuario que inció sesión	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/contextmenu/detailedprofile.aspx
1.10.49			Email Profile: debe incluir: Asunto del correo/Message ID/Risk level/Fecha y hora del correo/Dirección de remitente/dirección de destinatarios/Información de cada adjunto al correo/URLs embebidas/Cabecera del correo	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/contextmenu/detailedprofile.aspx

1.10.50			Despliega el análisis de causa raíz y provee información adicional que puede ser útil para la investigación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain.aspx
1.10.51			- Debe desplegar un análisis visual de los objetos envueltos en un evento	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/executionprofile.aspx
1.10.52			Debe resaltar los objetos en la cadena que son posiblemente maliciosos	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/executionprofile.aspx
1.10.53			Debe desplegar el objeto o la lista de objetos que coinciden con los criterios de investigación definidos	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysis-ac/objectdetails.aspx
1.10.54			Debe resaltar el objeto "mas probable" que creó el objeto que coincidió con el criterio de investigación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysis-ac/objectdetails.aspx

1.10.55			Debe desplegar detalles del endpoint que fue investigado	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain.aspx
1.10.56			La cadena de análisis debe usar iconos para los distintos tipos de objetos (servidor/endpoint/url/archivos, etc...). La descripción debe estar directamente en la ventana de investigación para entender rápidamente la relación entre los distintos objetos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain/root-causeanalysis-.aspx
1.10.57			Debe poder obtenerse una representación visual de correlación de eventos de la perspectiva de la red y no del endpoint.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
1.10.58			Network Analytics debe usar como sensor al BDS (Breach Detection System) y debe proveer integración nativa para compartir no solo eventos sino el contexto entero (toda la telemetría posible).	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/overview-of-thenetw.aspx
1.10.59			Debe tener una barra de reproducción (play/pause) con un "time slider" para ver eventos correlacionados vs tiempo	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-

					c_001.aspx
1.10.60			Cada gráfica de correlación debe tener 1 o más líneas de correlación que muestran actividad maliciosa o sospechosa entre un origen y destino.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
1.10.61			Cada línea de correlación representa 1 o más transacciones entre 2 hosts.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
1.10.62			El grosor de la línea es proporcional al número de transacciones entre los hosts. Al colocar el mouse sobre la línea debe mostrar el número de transacciones para esa línea de correlación	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
1.10.63			La líneas de correlación debe poder ser entre host interno y externo. También debe poder ser entre 2 hosts internos (para identificar movimientos laterales).	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx

1.10.64			Cada línea de correlación debe indicar los protocolos usados. Y debe existir una flecha para indicar direccionalidad de la comunicación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
1.10.65			Debe identificar actividades claves para hosts internos y externos en la gráfica.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
1.10.66			Debe incluir actividades similares a: Machine Learning, Lateral Activity, Detected Event, C&C Activity, and Malicious Download.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
1.10.67			Correlation Information Pop-up Window: Debe incluir los sigueintes campos: Source IP/Destination IP/Severity/URLs/Hashes/Protocols/Number of transactions/Reason/Earliest date/Latest date	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/reviewing-thesummar_001.aspx
1.10.68			Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/responsemanagement.aspx

1.10.69			Debe responder a amenazas sin dejar la consola de XDR.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/responsemanagement/response-actions.aspx
1.10.70			Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos. Añadir a lista de bloqueo Eliminar de lista de bloqueo Terminar procesos en endpoints Recolectar archivos en endpoints Bloquear remitente de correo Poner en cuarentana un correo Borrar un correo Aislar un equipo Restaurar la conexión en equipos aislados	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/responsemanagement/response-actions.aspx
1.10.71			Después de activar la respuesta a un evento u objeto, debe poderse ver el estado de la tarea de respuesta y los detalles de comando en una tabla de Gestión de Respuesta	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/responsemanagement.aspx
1.10.72			Debe permitir realizar barridos IoC, personalizar búsquedas por especificación de parámetros, filtros y otros criterios y búsqueda de múltiples eventos que ocurraen en un mismo Endpoint	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence-/intelligencereports/sweeping.aspx
1.10.73			Debe tener un constructor de peticiones que debe permitir combinar atributos de búsqueda, operadores y especificar valores en una misma petición de búsqueda	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
1.10.74			Debe listar busquedas previas	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx

1.10.75			Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx
1.10.76			El administrador debe poder ver los queries guardados	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx
1.10.77			Debe ser fácil limpiar los criterios de búsqueda	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/searchactions.aspx
1.10.78			Los resultados deben ser exportables a CSV o JSON	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/savedqueries.aspx
1.10.79			Los resultados deben mostrar origen de los datos (workstation/servidor/email/network)	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/data-mappingintro/data-mappingsdl.aspx
1.10.80			El administrador debe ser capaz de ver los logs en RAW	SI	https://success.trendmicro.com/solution/000282728
1.10.81			debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado en Kibana para identificar, categorizar y obtener los resultados de búsqueda.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx

1.10.82			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: SAML Single Sign-On Account Management Role Management Product Connector Alert Notifications Audit Logs Remote Support	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/administrativesetti/administration.aspx
1.11.1		GARANTIA	soporte directo de fabricante con una disponibilidad 7x24 para atención de incidentes y contar con actualizaciones de software por la vigencia del contrato	SI	Technology Partners documento de servicio CVC
1.11.2			Soporte directo de fabricante para la atención de incidentes de forma remota por medio de correo electrónico y telefónico.	SI	Technology Partners documento de servicio CVC
1.11.3			El fabricante deberá contar con un servicio de laboratorio de investigación en español para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones hispanohablantes	SI	Technology Partners documento de servicio CVC https://docs.trendmicro.com/all/smb/wfbs-a/v7.0/en us/wfbsa_7.0_olh/WFBS/Managing_Updates/about_activeupdate.htm
ITEM	**LICENCIAMIENTO**	**ESPECIFICACIÓN**	**DESCRIPCIÓN**		
2	licencias para asociar a plataforma XDR	MARCA	TREND MICRO	SI	
2.1.1		VERSIÓN	Licencias software cloud XDR para endpoint TREND MICRO XDR	SI	
2.1.2		CANTIDAD	166	SI	
2.2.1		Sistemas Operativos soportados	Windows 7 (32-bit / 64-bit) Service Pack 1	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-.aspx

					https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/trendmicrosupporte.aspx
2.2.2			Windows 8.1 (32-bit / 64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-online help/intro-and-gspart/trend-microxdrabou_001/trendmicrosupporte.aspx
2.2.3			Windows 10 (32-bit / 64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/trendmicrosupporte.aspx
2.2.4			Windows Server 2008 R2 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/trendmicrosupporte.

					aspx
2.2.5			Windows MultiPoint Server 2010 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/trendmicrosupporte.aspx
2.2.6			Windows MultiPoint Server 2011 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/trendmicrosupporte.aspx
2.2.7			Windows Server 2012 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx
2.2.8			Windows Server 2016 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/

					officescanagent-sys/freshinstallations-_001.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/trendmicrosupporte.aspx
2.2.9			Windows Server 2019 (64-bit)	SI	https://docs.trendmicro.com/enus/enterprise/apexone-as-a-serviceonlinehelp/officescanagentdep/officescanagentins/officescanagent-sys/freshinstallations-_001.aspx https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/trend microsupporte.aspx
2.3.1		PLATAFORMA XDR	Debe permitir a la entidad tener la capacidad de detección y respuesta en email, endpoints, servidores, workloads en la nube y la red a través de una sola plataforma, es decir, poder hacer estas tareas de detección y respuesta en múltiples capas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.2			Debe proveer un mejor contexto y un análisis más profundo, para que la entidad pueda responder de forma más rápida y eficiente a amenazas, minimizando el impacto y alcance de un incidente en la organización	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.3			debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx

2.3.4			Los modelos de correlación deben combinar multiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.5			La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
2.3.6			Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench.aspx
2.3.7			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	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.8			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	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/workbenchdata.aspx
2.3.9			Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-.aspx
2.3.10			debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/alertdetails.aspx

2.3.11			Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las acciones que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain.aspx
2.3.12			Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalytics-re.aspx
2.3.13			Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx
2.3.14			Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/search-syntaxsimple.aspx
2.3.15			Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain.aspx
2.3.16			Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/savedqueries.aspx

2.3.17			Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence-/intelligencereports/curatedintelligence.aspx
2.3.18			La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana 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	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-bnlinehelp/xdrpart/observedattack-tech.aspx
2.3.19			Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-micro xdrabou_001/featuresand-benefit.aspx
2.3.20			En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.21			Debe ofrecer opciones de respuesta "context aware" para acciones rápida desde la plataforma.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.22			Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.23			Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx

2.3.24			Debe proveer un conector para Splunk nativo	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.25			Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.26			debe analizar la data recolectada por los sensoress para proveer alertas inteligentes, y detecciones de alta fidelidad.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/securityposturegro/identity-andrisk-in/riskinsights/cloud-apprisk-index/xdrdetections.aspx
2.3.27			Los sensores deben soportar integración nativa del vendor para obtener toda la data de actividad (telemetria, metadata, netflow) no solo data de alertas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.28			Los sensores deben soportar trabajar al menos en los siguientes sistemas operativos de Estaciones de trabajo de usuarios: Windows 7 y superior Mac OS X El Capitan 10.11 y superior	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/inventorymanagement_001/endpoint-inventory-2/xdr-sensorsupported.aspx

2.3.29			Los sensores deben soportar trabajar al menos en las siguientes sistemas operativos de servidores Windows (Windows 2008 y superiqr) Linux (Including visibility over docker containers attacks) Red Hat Enterprise Linux 6 y superior Ubuntu 16 y superior CentOS 6 y superior Debian 8 y superior Amazon Linux/Amazon Linux 2 Oracle Linux 6 y superior SUSE Linux Enterprise Server 12 y superior CloudLinux 7 y superior	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/inventorymanagement_001/endpoint-inventory-2/xdr-sensorsupported.aspx
2.3.30			Los sensores deben soportar trabajar por integración directa vía API con los proveedores de correo Microsoft 365 & G Suite	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/inventorymanagement_001/endpoint-inventory-2/xdr-sensorsupported.aspx
2.3.31			Los sensores deben soportar trabajar Network por integración nativa con sistema BDS	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdr-abou_001.aspx
2.3.32			En el caso de estaciones de trabajo de usuarios y servidores, la funcionalidad XDR debe ser una capacidad que puede tener embebida en el mismo agente de protección de endpoint. XDR no debe ser un agente adicional	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.33			Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
2.3.34			El vendor debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos to improve.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-

					benefit.aspx
2.3.35			Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/incident-view.aspx
2.3.36			El aplicativo de Detection Model Management debe permitir controlar el tipo de alertas que se disparan y se envían a Workbench.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
2.3.37			Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE. Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen. High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen. Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
2.3.38			Los modelos deben especificar para que productor en específico (Workstation/Server/Email/Network) aplica una alerta	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
2.3.39			Los modelos deben especificar y permitir modificar "status": encendido/apagado	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx

2.3.40			Los modelos deben especificar la ultima vez que se actualizó	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/detectionmodels.aspx
2.3.41			Debe hacer una sección de excepciones dentro de la App de Model Management que despliegue todas las excepciones que se añadieron.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detection modelmana/exceptions.aspx
2.3.42			La excepcion debe ser granular y debe mostrar lo siguiente: Object: El objeto que se ha añadido como excepción en una investigación Filter: El filtro que identificó el objeto como un indicador de amenaza Type: El atributo del objeto añadido Data field: Log definido por el objeto Match type: Exacto o Parcial (soporta wildcards) Description: Información definida por el usuario para la excepción Created: Fecha y hora en que se añadió la excepción Created by: Usuario que creó la excepción	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
2.3.43			Debe permitir añadir excepciones durante la investigación de una alerta.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
2.3.44			En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/detectionmodelmana/exceptions.aspx
2.3.45			Debe integrar inteligencia al minuto con reportes del vendor y terceras partes confiables para ayudar a identificar amenazas	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence-/intefligencereports/curatedintelligence.

					aspx
2.3.46			Debe poder analizar los logs, comparar la data contra los reportes de Threat Intelligence automáticamente, y generar alertas basadas en indicadores sospechosos o maliciosos detectados	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence/intelligencereports.aspx
2.3.47			La App de Workbench debe mostrar alertas por los modelos de detección y permitir investigar a más detalle. La data del Workbench debe incluir: Status: New/In Progress/Closed/Closed – False Positive Score: basado en la severidad del modelo de detección y el impacto de la alerta. Workbench ID: identificador único para la alerta Model: Modelo que disparó la alerta Model severity: Severidad asignada al modelo que disparó la alerta Impact scope: Número de entidades afectadas por Servers/Workstations/Users/Cuentas de correo Created: Fecha y Hora que XDR generó la alerta	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/workbenchdata.aspx
2.3.48			Endpoint Profile: Debe incluir Hostname/IPv4/GUID/MAC Address/OS version/Producto/Último usuario que inció sesión	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performinganalert-/contextmenu/detailedprofile.aspx
2.3.49			Email Profile: debe incluir: Asunto del correo/Message ID/Risk level/Fecha y hora del correo/Dirección de remitente/dirección de destinatarios/Información de cada adjunto al correo/URLs embebidas/Cabecera del correo	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performinganalert-/contextmenu/detailedprofile.aspx

2.3.50			Despliega el análisis de causa raíz y provee información adicional que puede ser útil para la investigación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain.aspx
2.3.51			Debe desplegar un análisis visual de los objetos envueltos en un evento	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/executionprofile.aspx
2.3.52			Debe resaltar los objetos en la cadena que son posiblemente maliciosos	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/executionprofile.aspx
2.3.53			Debe desplegar el objeto o la lista de objetos que coinciden con los criterios de investigación definidos	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysis-ac/objectdetails.aspx
2.3.54			Debe resaltar el objeto "mas probable" que creó el objeto que coincidió con el criterio de investigación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysis-ac/objectdetails.aspx

2.3.55			Debe desplegar detalles del endpoint que fue investigado	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain.aspx
2.3.56			La cadena de análisis debe usar Iconos para los distintos tipos de objetos (servidor/endpoint/url/archivos, etc...). La descripción debe estar directamente en la ventana de investigación para entender rápidamente la relación entre los distintos objetos.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/analysischain/root-causeanalysis-.aspx
2.3.57			Debe poder obtenerse una representación visual de correlación de eventos de la perspectiva de la red y no del endpoint.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
2.3.58			Network Analytics debe usar como sensor al BDS (Breach Detection System) y debe proveer integración nativa para compartir no solo eventos sino el contexto entero (toda la telemetría posible).	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/overview-of-thenetw.aspx
2.3.59			Debe tener una barra de reproducción (play/pause) con un "time slider" para ver eventos correlacionados vs tiempo	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-

					c_001.aspx
2.3.60			Cada gráfica de correlación debe tener 1 o más líneas de correlación que muestran actividad maliciosa o sospechosa entre un origen y destino.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performing an-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
2.3.61			Cada línea de correlación representa 1 o más transacciones entre 2 hosts.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
2.3.62			El grosor de la línea es proporcional al número de transacciones entre los hosts. Al colocar el mouse sobre la línea debe mostrar el número de transacciones para esa línea de correlación	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
2.3.63			La línea de correlación debe poder ser entre host interno y externo. También debe poder ser entre 2 hosts internos (para identificar movimientos laterales).	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx

2.3.64			Cada línea de correlación debe indicar los protocolos usados. Y debe existir una flecha para indicar direccionalidad de la comunicación.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
2.3.65			Debe identificar actividades claves para hosts internos y externos en la gráfica.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
2.3.66			Debe incluir actividades similares a: Machine Learning, Lateral Activity, Detected Event, C&C Activity, and Malicious Download.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/analysis-usingthe-c_001.aspx
2.3.67			Correlation Information Pop-up Window: Debe incluir los sigueintes campos: Source IP/Destination IP/Severity/URLs/Hashes/Protocols/Number of transactions/Reason/Earliest date/Latest date	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/xdrpart/workbench/alert-view/performingan-alert-/advancedanalysisac/networkanalyticsre/reviewing-thesummar_001.aspx
2.3.68			Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/responsemanagement.aspx

2.3.69			Debe responder a amenazas sin dejar la consola de XDR.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonappe/responsemanagement/response-actions.aspx
2.3.70			Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos. Añadir a lista de bloqueo Eliminar de lista de bloqueo Terminar procesos en endpoints Recolectar archivos en endpoints Bloquear remitente de correo Poner en cuarentana un correo Borrar un correo Aislar un equipo Restaurar la conexión en equipos aislados	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonappe/responsemanagement/response-actions.aspx
2.3.71			Después de activar la respuesta a un evento u objeto, debe poderse ver el estado de la tarea de respuesta y los detalles de comando en una tabla de Gestión de Respuesta	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/responsemanagement.aspx
2.3.72			Debe permitir realizar barridos IoC, personalizar búsquedas por especificación de parámetros, filtros y otros criterios y búsqueda de múltiples eventos que ocurraen en un mismo Endpoint	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/threatintelligence-/intelligencsreports/sweeping.aspx
2.3.73			Debe tener un constructor de peticiones que debe permitir combinar atributos de búsqueda, operadores y especificar valores en una misma petición de búsqueda	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/intro-and-gspart/trend-microxdrabou_001/featuresand-benefit.aspx
2.3.74			Debe listar busquedas previas	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonappe/searchapp.aspx

2.3.75			Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx
2.3.76			El administrador debe poder ver los queries guardados	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx
2.3.77			Debe ser fácil limpiar los criterios de búsqueda	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/searchactions.aspx
2.3.78			Los resultados deben ser exportables a CSV o JSON	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/savedqueries.aspx
2.3.79			Los resultados deben mostrar origen de los datos (workstation/servidor/email/network)	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp/data-mappingintro/data-mappingsdl.aspx
2.3.80			El administrador debe ser capaz de ver los logs en RAW	SI	https://success.trendmicro.com/solution/000282728
2.3.81			debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado en Kibana para identificar, categorizar y obtener los resultados de búsqueda.	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/commonapps/searchapp.aspx

2.3.82			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: SAML Single Sign-On Account Management Role Management Product Connector Alert Notifications Audit Logs Remote Support	SI	https://docs.trendmicro.com/enus/enterprise/trendmicro-xdr-onlinehelp/administrativesetti/administration.aspx
2.4.1		GARANTIA	soporte directo de fabricante con una disponibilidad 7x24 para atención de incidentes y contar con actualizaciones de software por la vigencia del contrato	SI	Technology Partners documento de servicio CVC
2.4.2			Soporte directo de fabricante para la atención de incidentes de forma remota por medio de correo electrónico y telefónico.	SI	Technology Partners documento de servicio CVC
2.4.3			El fabricante deberá contar con un servicio de laboratorio de investigación en español para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones hispanohablantes	SI	Technology Partners documento de servicio CVC https://docs.trendmicro.com/all/smb/wfbs-a/v7.0/enus/wfbsa_7.0_olh/WFBS/Managing_Updates/about_activeupdate.htm

Obligaciones del Contratista: Los licenciamientos entregados deberán contar con una vigencia y garantía de mínimo un (1) año, prestada directamente por el fabricante.

- **Con respecto a la entrega e instalación de licenciamientos en los equipos de cómputo de la entidad**

- Aplicar las políticas de seguridad establecidas por la entidad
- La actualización de patrones y de la plataforma será por parte del proveedor de la solución
- Adjuntar a su oferta una carta emitida por el fabricante o mayorista, en donde se certifica que tiene la experiencia suficiente para la instalación y soporte de las soluciones ofertadas y que se encuentra autorizado para comercializarlas en el territorio colombiano
- El proveedor de la solución debe disponer de mínimo 1 ingeniero certificado por el fabricante en las soluciones ofertadas

- Hacer la validación de activación y acceso a la consola de administración de la solución y garantizar el correcto registro de licenciamiento contratado
- Realizar la configuración de las reglas, perfiles y políticas de seguridad de equipo de usuario final en la consola de administración de la solución y asegurar que cumplan las funciones (protección antimalware, DLP, control de aplicaciones, protección web) que actualmente cumple la solución existente.
- Realizar y validar la integración y sincronización de la consola de administración de la solución con el directorio activo de la CVC, para aplicar políticas de seguridad de equipo final basadas en roles de usuarios corporativos.
- Realizar la configuración de 5 reportes de seguridad usando las herramientas disponibles en la consola de administración de la solución
- Activar y realizar la integración del producto de protección de antivirus con la plataforma de XDR en nube
- Entregar la transferencia de conocimientos para los ingenieros de la entidad
- Realizar el proceso de desinstalación de agentes de antivirus a 836 equipos de la Corporación
- Realizar el proceso de instalación de agentes en 836 endpoint de manera remota y sincronización remota a la plataforma XDR de 166 equipos de cómputo que actualmente cuentan con solución de protección de endpoint en la institución.
- Acordar con el Supervisor los tiempos de desinstalación e instalación de los agentes de software y el método de contacto de los usuarios.

TECHNOLOGY PARTNERS S.A.S. entiende, acepta y certifica que cumple con los requerimientos exigidos en el presente proceso de Selección Abreviada Menor Cuantía no. 38 – 2021, con respecto a Anexo Técnico 1, evidenciado en el documento ANEXO 1 TECNICO SAMC 38 DE 2021 TECHNOLOGY PARTNERS.pdf

EVALUACION FINAL DE PROPUESTAS

Ponderación para la modalidad del proceso de Licitación Pública: Para determinar la oferta más favorable la CVC tendrá en cuenta la ponderación de los elementos de calidad y precio, soportados en puntajes y/o formulas.

FACTOR	CRITERIOS DE PONDERACION	PUNTAJE
Económico	Precio (fórmula)	40 puntos
Técnico	Calidad (puntaje)	60 puntos
Total		**100 Puntos**

* Incentivos a la industria nacional y Proponentes con trabajadores discapacitados

Factor Económico - Precio: Se asignará un puntaje máximo de 40, aplicando como método de cálculo del puntaje para el factor precio la Media Geométrica con Presupuesto Oficial, consiste en establecer la media geométrica de las Ofertas válidas y el presupuesto oficial un número determinado de veces y la asignación de puntos en función de la proximidad de las Ofertas a dicha media geométrica, como resultado de aplicar las fórmulas que se indican en seguida. Para el cálculo de la media geométrica con

presupuesto oficial se tendrá en cuenta el número de Ofertas válidas y se incluirá el presupuesto oficial del Proceso de Contratación en el cálculo tantas veces como se indica en el siguiente cuadro:

Número de propuestas (n)	Número de veces en las que se incluye el presupuesto oficial (nv)
1 a 3	1
4 a 6	2
7 a 9	3
10 a 12	4
13 a 15	5
.....	.....

Y así sucesivamente por cada tres propuestas válidas se incluirá una vez el presupuesto oficial del proceso de contratación.

Seguidamente se determinará la media geométrica con la inclusión del presupuesto oficial de acuerdo a lo establecido en el cuadro anterior mediante la siguiente fórmula:

$$MGPO \quad \sqrt[(nv+n)]{PO * PO * \cdots POnv * P1 * P2 * \cdots Pn}$$

$$\sqrt[(nv+n)]{PO * PO * \cdots POnv * P1 * P2 * \cdots Pn}$$

Dónde:

MGPO = Media geométrica con presupuesto oficial.
N = Número de propuestas válidas.
nv = Número de veces que se incluye el presupuesto oficial (PO).
PO = Presupuesto oficial.
Pn = Valor de la propuesta económica corregida del proponente i.

Obtenida la media geométrica con presupuesto oficial se procederá a ponderar las propuestas de acuerdo con la siguiente formula.

$$\text{Puntaje i para valores menores o iguales a MGPO= 600} \times \left[1 - \left[\frac{MGPO - Vi}{MGPO}\right]\right]$$

$$\text{Puntaje i para valores mayores a MGPO= 600} \times \left[1 - 2\left[\frac{|MGPO - Vi|}{MGPO}\right]\right]$$

Donde
MGPO = Media geométrica con presupuesto oficial
Vi = Valor total corregido de cada una de las propuestas i
i = Número de propuesta

En el caso de propuestas económicas con valores mayores a la media geométrica con presupuesto oficial se tomará el valor absoluto de la diferencia entre la media geométrica con presupuesto oficial y el valor de la propuesta, como se observa en la fórmula de ponderación.

En todo caso, cuando el valor de la propuesta supere el presupuesto oficial establecido, aplicará causal de rechazo contenida en el pliego de condiciones.

Evaluación

Conforme a lo consignado en el FORMULARIO No. 1, se tiene:

- Valor del presupuesto oficial de Selección Abreviada menor cuantía No. 38 – 2021: CIENTO SESENTA Y UN MILLONES CUATROCIENTOS OCHENTA Y CINCO MIL CIENTO CINCUENTA Y SEIS PESOS MONEDA CORRIENTE ($161.485.156) IVA INCLUIDO 19%.

- Valor ofertado por el proponente TECHNOLOGY PARTNERS S.A.S.: CIENTO SESENTA MILLONES NOVECIENTOS OCHENTA MIL OCHOCIENTOS CINCUENTA Y TRES PESOS MONEDA CORRIENTE MCTE. ($160.980.853) IVA INCLUIDO 19%.

Dado que TECHNOLOGY PARTNERS S.A.S., es el único proponente habilitado y, además, el valor total de su propuesta no supera el valor total presupuestado para el presente proceso de Selección Abreviada menor cuantía, se le asigna el puntaje máximo para el presente ítem, correspondiente a **cuarenta (40) puntos**.

EVALUACIÓN FACTOR DE CALIDAD (60 PUNTOS):

Se asignará un puntaje máximo de 60 puntos al proponente que oferte: Una (1) Capacitación virtual para la mesa de ayuda de la corporación de ocho (8) horas, orientada a la implementación y soporte técnico de los clientes antivirus.

Corporación Autónoma Regional del Valle del Cauca

Lo cual se acreditará mediante una carta firmada por el representante legal del oferente, donde se compromete a dictar estrictamente la capacitación señalada.

EVALUACION:

La empresa **TECHNOLOGY PARTNERS S.A.S.** certifica que brindara una (1) Capacitación virtual para la mesa de servicio integral de la corporación de ocho (8) horas, orientada a la implementación y soporte técnico de los clientes antivirus, evidenciado en FORMATO No 7. Por lo anterior se asignan 60 puntos.

Calificación Final:

Como resultado de los numerales anteriores se obtiene la siguiente calificación:

1. Calidad	60
2. Precio	40

El puntaje total obtenido en la evaluación de calidad y precio, por parte de la firma **TECHNOLOGY PARTNERS S.A.S.**, corresponde a cien (100) puntos, adicional mente se otorgan 10 puntos por concepto de Promoción de servicios nacionales o con trato nacional quedando con ***110 puntos.***

5. CONCLUSIÓN DE LA EVALUACIÓN

Luego de efectuada la evaluación sobre los criterios de Calidad, y Precio (valor total de la propuesta), de acuerdo con la propuesta presentada por la firma **TECHNOLOGY PARTNERS S.A.S.**, obtiene un puntaje de ciento diez (110) puntos, conforme a lo estipulado en el Pliego de Condiciones Definitivo de Selección Abreviada menor cuantía No. 38 – 2021, por lo cual puede continuar con el proceso para una eventual adjudicación.

Para constancia, se firma el día veintiuno (21) de diciembre de 2021, en la ciudad de Santiago de Cali.