UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

ESPECIFICACIONES TÉCNICAS

SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA ANTE CIBERAMENAZAS

PROGRAMA RED UDNET

Contenido

Especificaciones técnicas

1. **Objeto del proceso**

   Adquirir una solución de detección, prevención y respuesta ante ciberamenazas a nivel de red, que garantice la administración y analítica de tráfico centralizada, integración con la infraestructura de seguridad actual de la Universidad, capacidades de visibilidad, monitoreo y correlación de eventos para endpoints estratégicos, incluyendo los componentes de hardware y software necesarios para su implementación, configuración y operación on premise, soporte técnico especializado 7x24 y garantía.

2. **Alcance técnico**

   a. **Suministro de hardware:** Componentes físicos necesarios para la correcta implementación y operación de la solución ofertada (servidores, appliances, sensores, interfaces de captura, módulos, cableados y demás elementos requeridos según la solución del oferente).

      La arquitectura prevista para la implementación de la solución debe contemplar un nodo (físico) central de administración y análisis ubicado en la sede Calle 40 de la Universidad Distrital y un sensor o colector de tráfico (físico) en la sede Bosa Porvenir. Además, con el fin de fortalecer las capacidades de monitoreo y análisis de tráfico de red sobre los segmentos priorizados por la Universidad, debe permitir la incorporación de nuevos sensores, los cuales podrán ser desplegados de manera virtual o física sobre la infraestructura tecnológica de la Universidad, sin que ello genere costos adicionales la Universidad.

      El hardware propuesto deberá permitir el almacenamiento, consulta de eventos, alertas y telemetría histórica generada por la solución, garantizando una retención mínima de noventa (90) días disponibles para análisis por parte de la Universidad.

   b. **Suministro de licenciamiento:** Licenciamiento de una solución de detección, prevención y respuesta ante ciberamenazas a nivel de red, bajo arquitectura On-Premise, por un periodo mínimo de un (1) año, incluyendo el derecho a actualizaciones (updates y upgrades) durante la vigencia del licenciamiento.

      La solución deberá permitir complementar las capacidades actuales de seguridad de la Universidad mediante funcionalidades de administración y analítica centralizada de tráfico de red, visibilidad sobre comunicaciones norte-sur y este-oeste, correlación de eventos de seguridad e integración con las herramientas de seguridad y monitoreo existentes en la infraestructura institucional.

      La solución deberá incluir capacidades de visibilidad, monitoreo y correlación de eventos para cuatrocientos (400) endpoints, por un periodo mínimo de un (1) año, como complemento a las capacidades de detección y respuesta de red de la solución ofertada, sin constituir una solución independiente de Endpoint Detection and Response (EDR).

      Estas capacidades deberán permitir la recolección y envío de telemetría, metadatos y contexto de seguridad hacia la plataforma central de administración y análisis ofertada, incluyendo información relacionada con conexiones de red, actividad sospechosa, eventos de seguridad y

comportamiento de los equipos monitoreados, mediante agentes, sensores, telemetría de red u otros mecanismos soportados por el fabricante.

Teniendo en cuenta que la arquitectura propuesta contempla la implementación de un nodo central de administración y análisis en la sede Calle 40 y el despliegue de sensores de monitoreo de tráfico en la sede Bosa Porvenir, la solución deberá complementar las capacidades de visibilidad sobre equipos estratégicos ubicados en otras sedes, segmentos de red o escenarios donde el tráfico no transite directamente por los puntos de captura implementados. Estas capacidades deberán ser compatibles e interoperables con las herramientas de protección de endpoints existentes en la infraestructura tecnológica de la Universidad.

c. Implementación: Instalación, configuración y puesta en correcto funcionamiento de la solución (hardware y software), incluyendo el despliegue de sensores o colectores de tráfico en las sedes Calle 40 Bosa Porvenir, de acuerdo con la arquitectura de despliegue propuesta (On-Premise).

El contratista deberá garantizar la correcta integración con la red existente, la configuración de mecanismos de captura o espejo de tráfico (SPAN, port mirroring o equivalentes), así como la realización de pruebas de funcionamiento que permitan evidenciar la correcta operación de la solución.

El contratista deberá acompañar las actividades de estabilización y puesta en producción de la solución, garantizando su correcta operación e integración con la infraestructura institucional previo al cierre del proceso de implementación.

d. Integración: Configuración e integración de la solución con las herramientas de seguridad y monitoreo existentes en la Universidad Distrital, con el fin de facilitar la correlación de eventos y la automatización de acciones de respuesta ante incidentes de seguridad, incluyendo:

- **Firewall de Palo Alto Networks (NGFW 3420):** Integración para el bloqueo automático de direcciones IP maliciosas y la ejecución de acciones de contención a nivel de red.
- **EDR de Kaspersky (versión 12.11 y agente 16.1):** Integración para la correlación de eventos y la ejecución de acciones de respuesta en los endpoints.
- **Plataforma de monitoreo de red SolarWinds:** Integración para el aprovechamiento de la información de monitoreo de red y la generación de alertas que puedan ser correlacionadas en el SIEM institucional SolarWinds Security Event Manager (SEM), licenciamiento actual SEM50, anteriormente conocido como LEM.

e. Soporte, mantenimiento y actualizaciones: El servicio deberá prestarse mediante atención remota (correo electrónico o sistema de tickets), telefónica y, cuando sea requerido, atención en sitio de acuerdo con la criticidad del incidente. El contratista deberá garantizar soporte técnico especializado en esquema 7x24 durante un periodo mínimo de un (1) año, contado a partir de la puesta en correcto funcionamiento de la solución.

Durante este periodo se deberán garantizar las actualizaciones permanentes de la solución, incluyendo updates y upgrades.

El contratista deberá realizar actividades de mantenimiento preventivo y correctivo orientadas a garantizar la continuidad operativa de la plataforma, incluyendo revisión de componentes, optimización de configuraciones, validación de integraciones y generación de reportes técnicos de las actividades realizadas.

Todas las actividades de mantenimiento y actualización deberán ser coordinadas previamente con la supervisión del contrato.

f. Transferencia de conocimiento: Ejecución de actividades de capacitación técnica y transferencia de conocimiento dirigidas al personal designado por la Supervisión, orientadas a la administración, monitoreo y operación de la solución implementada.

La capacitación deberá contemplar una intensidad de al menos doce (12) horas e incluir, como mínimo, temas relacionados con la arquitectura de la solución, administración de la plataforma, análisis y gestión de alertas, procedimientos básicos de respuesta a incidentes y buenas prácticas de operación. En este sentido, el contratista deberá suministrar la documentación técnica y el material de apoyo correspondiente.

Nota: Los requerimientos técnicos mínimos se describen con mayor detalle en el numeral 4 del presente documento.

3. Descripción del contexto técnico

La Universidad Distrital Francisco José de Caldas cuenta con una infraestructura tecnológica conformada por equipos de cómputo (portátiles y de escritorio), servidores físicos y virtuales, así como diversos servicios institucionales críticos que soportan los procesos académicos, administrativos y de investigación de la comunidad universitaria. Dicha infraestructura se encuentra distribuida en diferentes sedes y centros de datos institucionales, y soporta múltiples plataformas tecnológicas y sistemas operativos que permiten la operación de servicios académicos, administrativos, sistemas de información institucionales, servicios web, bases de datos y plataformas de apoyo a la docencia e investigación.

Actualmente, 4.000 equipos del parque informático cuentan con el software de seguridad Kaspersky® Next EDR Optimum instalado y en funcionamiento. Estas soluciones han protegido los dispositivos frente a amenazas como backdoors, rootkits, troyanos, keyloggers, spyware, virus y demás tipos de malware, contribuyendo a garantizar la confidencialidad, integridad y disponibilidad de la información institucional. Los equipos servidores, PC y portátiles han contado con protección de Kaspersky desde el 13 de agosto de 2008, cuyo licenciamiento se ha adquirido mediante contratos trianuales.

En materia de seguridad informática, la Universidad dispone además de soluciones de seguridad perimetral basadas en firewalls de próxima generación Palo Alto Networks modelo 3420 en esquema de alta disponibilidad (HA), así como de la plataforma SolarWinds para el monitoreo de infraestructura y red y la gestión de eventos de seguridad mediante SolarWinds Security Event Manager (SIEM), actualmente licenciado y en operación. Estas soluciones permiten la inspección de tráfico, la generación de alertas y la correlación de eventos de seguridad.

No obstante, actualmente la infraestructura tecnológica opera con un nivel de integración parcial entre las diferentes plataformas de seguridad y monitoreo, lo que limita la correlación centralizada de eventos, el análisis avanzado del tráfico de red y la posibilidad de implementar mecanismos automatizados de respuesta coordinada frente a incidentes de seguridad informática.

Adicionalmente, la creciente sofisticación de amenazas avanzadas, ataques dirigidos, movimientos laterales dentro de la red y técnicas de evasión hace necesario fortalecer las capacidades institucionales de detección, prevención y respuesta frente a ciberamenazas a nivel de red.

En este contexto, se hace necesaria la adquisición de una solución de detección, prevención y respuesta ante ciberamenazas a nivel de red, implementada bajo arquitectura On-Premise, que incluya los componentes de hardware y software requeridos para su implementación, configuración, puesta en funcionamiento y operación dentro de la infraestructura tecnológica de la Universidad Distrital Francisco José de Caldas, así como el soporte técnico especializado en esquema 7x24, garantía y el derecho a actualizaciones (updates y upgrades) durante la vigencia del licenciamiento.

4. Requerimientos técnicos mínimos obligatorios

La solución a adquirir deberá cumplir con los requerimientos técnicos mínimos orientados a asegurar capacidades avanzadas de monitoreo, visibilidad, detección de amenazas, análisis de comportamiento, correlación de eventos, generación de alertas y respuesta ante incidentes, integración con la infraestructura tecnológica existente, así como soporte técnico especializado en esquema 7x24, incluyendo el derecho a actualizaciones (updates y upgrades) durante la vigencia del contrato, bajo una arquitectura de despliegue On-Premise.

Ítem	Característica técnica	Descripción
1	Arquitectura y componentes físicos de la solución	El oferente deberá dimensionar los equipos para el nodo central (Calle 40) y el sensor o colector de tráfico (Bosa Porvenir) garantizando que soporten la totalidad de la solución. Para la validación de este ítem se revisará la ficha técnica del hardware y software enviada por el oferente.
2	Arquitectura y componentes físicos de la solución	La solución deberá contemplar los componentes físicos necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura On-Premise.
3	Arquitectura y componentes físicos de la solución	La solución deberá incluir los componentes físicos necesarios para la implementación de un nodo central de administración, análisis y correlación de eventos, el cual deberá ser instalado en la sede Calle 40 y un sensor o colector de tráfico en la sede Bosa Porvenir
4	Arquitectura y componentes físicos de la solución	La solución deberá permitir la creación e incorporación de nuevos sensores, los cuales podrán ser desplegados de manera física o virtual sobre la infraestructura tecnológica de la Universidad, sin que ello genere costos adicionales la Universidad.
5	Arquitectura y componentes físicos de la solución	La solución deberá permitir escalabilidad para la incorporación futura de nuevos sensores, colectores o capacidades de procesamiento sin requerir el reemplazo total de la solución.
6	Arquitectura y componentes físicos de la solución	La solución deberá permitir el almacenamiento y consulta de eventos, alertas, registros y telemetría histórica por un periodo mínimo de noventa (90) días, conforme a la arquitectura ofertada.

Ítem	Característica técnica	Descripción
7	Arquitectura y componentes físicos de la solución	Los componentes físicos suministrados deberán incluir los accesorios, interfaces, módulos, cableados y demás elementos necesarios para su correcta instalación y puesta en funcionamiento.
8	Arquitectura y componentes físicos de la solución	La solución deberá soportar mecanismos de captura de tráfico mediante SPAN, port mirroring o tecnologías equivalentes compatibles con la infraestructura institucional.
9	Arquitectura y componentes físicos de la solución	La arquitectura propuesta deberá permitir la integración y comunicación segura entre el nodo central y los sensores o colectores desplegados.
10	Arquitectura y componentes físicos de la solución	Especificaciones técnicas - Patch cord dúplex de fibra óptica LC/LC: • Debe contar con las siguientes características: 1. OM4 u OM5. 2. Longitud de Onda mínimo de 850/1300 nm. 3. Longitud 2.0 metros con conector LC-LC 4. Tipo: Uniboot ó Zip-cord 5. Cincuenta y Ciento Veinticinco micrones (50/125) µm. 6. Soportar 10G hasta 550 metros y 1Gbps hasta 1100 metros, certificados según el estándar IEEE 802.3ae. • Los conectores deben cumplir con los estándares de cableado como lo estipula la norma ANSI/TIA-568- 3-D • Deben ser probados para soportar velocidades de transmisión hasta de 10 Gb/s para enlaces de hasta 550m con una fuente de 850nm según los estándares IEEE 802.3ae 10 GbE. • Deben estar garantizado mínimo por 25 años. • El cable debe tener un retardante de fuego de alta calidad, libre de halógenos, no producir gases tóxicos, la chaqueta de la fibra debe ser del tipo (LSZH ó LSZH-3). • Estos deben ser elaborados por el mismo fabricante. • Deben ser originales de fábrica y precertificados por el fabricante como estipula la ANSI/TIA 568.3-D, deben venir en su bolsa original de empaque tal como salen de la fábrica. • Los elementos estarán identificados individualmente con el correspondiente logo de la prueba de laboratorio, de forma permanente. Serán certificados por UL ó CSA ó ETL, para garantizar que los elementos ofrecidos han sido avalados por estos laboratorios. Adicionalmente puede estár marcado con el número de la prueba de flamabilidad. • Debe tener ficha técnica del fabricante del producto, con número de parte donde se pueda verificar las especificaciones y parámetros de desempeño, a través de la página web del fabricante.
11	Arquitectura y componentes físicos de la solución	**Especificaciones técnicas - SFP +** • Fabricante: Cisco – Se solicita de este fabricante teniendo en cuenta que el Switch Core es de esta marca y uno diferente podría traer complicaciones en la garantía del Switch Core. • Formato: SFP-10G-SR • Velocidad: 10 Gbps • Tipo de enlace: Ethernet 10 Gigabit (10GBASE-SR) • Fibra: Multimodo (MMF) • Conector: LC dúplex • Longitud de onda: 850 nm • Alcance típico: Hasta 400 m (OM4)
12	Requisitos Generales	La solución deberá ser ofertada en su versión estable y soportada oficialmente por el fabricante al momento de la presentación de la oferta, incluyendo acceso a

Ítem	Característica técnica	Descripción
		actualizaciones, parches y mejoras durante la vigencia del licenciamiento. Se debe presentar una certificación en donde se compruebe de lo solicitado.
13	Requisitos Generales	La solución deberá permitir configuraciones orientadas a garantizar que la información analizada y los eventos de seguridad permanezcan bajo control y administración de la Universidad, conforme a las políticas institucionales de seguridad de la información.
14	Requisitos Generales	La solución deberá soportar el crecimiento progresivo de activos monitoreados dentro de la infraestructura institucional, garantizando capacidades de procesamiento, análisis y correlación acordes con las necesidades de la Universidad.
15	Requisitos Generales	La solución deberá ser compatible con entornos tecnológicos que incluyan sistemas operativos Windows, Linux y MacOS, permitiendo capacidades de visibilidad, monitoreo, análisis o correlación sobre dichos entornos mediante los mecanismos soportados por la solución ofertada.
16	Requisitos Generales	La solución deberá contar con capacidades de detección y respuesta a nivel de red (NDR), así como permitir la integración y correlación con soluciones de seguridad de endpoints (EDR) y mecanismos de análisis avanzado de amenazas mediante sandboxing, ya sea de forma nativa o mediante integraciones soportadas por el fabricante, con el fin de fortalecer las capacidades de visibilidad, detección y respuesta ante incidentes de seguridad.
17	Arquitectura y Diseño de la Plataforma	La solución debe contar con capacidades centralizadas de investigación y correlación de eventos que permitan analizar la telemetría de red y la información asociada a los activos monitoreados por la solución, incluyendo el análisis del tráfico de red relacionado con protocolos de correo electrónico cuando este sea visible a nivel de red.
18	Arquitectura y Diseño de la Plataforma	La solución debe permitir la centralización lógica del análisis de información, garantizando una visión consolidada de eventos y alertas, pudiendo desplegar sus componentes en uno o varios nodos según el diseño arquitectónico propuesto por el fabricante.
19	Arquitectura y Diseño de la Plataforma	Cada Centro de Análisis deberá soportar el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de alta capacidad (mínimo 6 Gbps de tráfico o superior), sin degradación del análisis ni pérdida de visibilidad.
20	Arquitectura y Diseño de la Plataforma	La solución deberá permitir esquemas de alta disponibilidad (HA) para los componentes críticos de administración, análisis y procesamiento, incorporando mecanismos de redundancia, failover y continuidad operativa que minimicen la interrupción del servicio ante fallos de hardware o software.
21	Arquitectura y Diseño de la Plataforma	La solución debe incluir una interfaz web para que los administradores gestionen y analicen los datos del sistema, incluyendo el seguimiento de incidentes, la monitorización del rendimiento del sistema y la configuración de sistema.
22	Arquitectura y Diseño de la Plataforma	La solución debe soportar despliegues sobre entornos virtualizados VMware ESXi, HyperV, KVM o tecnologías de virtualización equivalentes, permitiendo la implementación futura de componentes adicionales de análisis, sensores o colectores en diferentes sedes o segmentos de red de la Universidad.
23	Arquitectura y Diseño de la Plataforma	La solución debe proporcionar notificaciones por correo electrónico a los administradores cuando los componentes del sistema experimenten problemas operativos, incluyendo baja capacidad de almacenamiento, para garantizar una atención y resolución rápidas.
24	Administración de la Plataforma	La solución deberá permitir la administración centralizada de políticas, eventos, tareas y reportes mediante una consola unificada de gestión.
25	Administración de la Plataforma	La solución debe soportar mecanismos controlados para la descarga de actualizaciones mediante conexión directa o a través de servidores proxy con autenticación.
26	Administración de la Plataforma	La solución deberá contar con un modelo de control de acceso basado en roles (RBAC), que permita: • La creación de roles personalizados. • La asignación granular de permisos por módulo, funcionalidad y alcance (por dominio o unidad organizacional).

Ítem	Característica técnica	Descripción
		• La aplicación del principio de mínimo privilegio. • La delegación administrativa segmentada por unidades organizacionales. • La integración con servicios de directorio (LDAP/Active Directory). • El registro y auditoría de todas las acciones realizadas por los usuarios administradores. • La gestión centralizada de perfiles y políticas de acceso.
27	Administración de la Plataforma	La solución debe utilizar un canal seguro para la comunicación entre la consola y el administrador. También debe permitir la importación del certificado digital utilizado para asegurar el canal de comunicación.
28	Administración de la Plataforma	La solución debe soportar sincronización de tiempo con servidores NTP.
29	Administración de la Plataforma	La solución deberá soportar mecanismos de copia de seguridad y restauración de la configuración, políticas, eventos, registros y demás componentes críticos para la operación de la plataforma.
30	Administración de la Plataforma	La solución deberá registrar y auditar las acciones realizadas por los usuarios administradores sobre la plataforma, permitiendo su consulta y conservación para fines de trazabilidad y auditoría.
31	Administración de la Plataforma	La solución debe soportar actualizaciones del Centro de Análisis preservando las configuraciones existentes, bases de datos de incidentes, políticas y demás información crítica de operación, sin requerir reinstalaciones completas desde cero y minimizando la interrupción del servicio.
32	Integración	La solución debe integrarse con servicios de inteligencia de amenazas, ya sean en la nube o locales, proporcionados por el fabricante o por fuentes confiables de terceros, para realizar comprobaciones de reputación en tiempo real sobre indicadores de compromiso.
33	Integración	La solución deberá permitir capacidades locales o híbridas de consulta y almacenamiento de información de inteligencia de amenazas, incluyendo reputación de indicadores de compromiso (IoC), hashes, URLs o dominios, con el fin de fortalecer las capacidades de análisis y correlación de eventos dentro de la infraestructura institucional.
34	Integración	La solución debe permitir el acceso a plataformas analíticas de inteligencia de amenazas que proporcionen contexto ampliado sobre indicadores, infraestructura asociada y relaciones entre objetos.
35	Integración	La solución deberá proporcionar APIs o mecanismos de integración que permitan, como mínimo: • Iniciar acciones de remediación y respuesta en endpoints. • Obtención de datos de telemetría de endpoints para sistemas de terceros. • Acceso a información de alertas de aplicaciones para sistemas de terceros. • Enviar archivos para escanear y recuperar resultados de escaneo para sistemas de terceros.
36	Integración	La solución deberá permitir integración con mecanismos estándar de inspección y análisis de contenido (por ejemplo, ICAP u otros métodos equivalentes como API o integración nativa con dispositivos de seguridad).
37	Integración	La solución debe soportar el envío de alertas de ciberseguridad y la monitorización de información mediante syslog.
38	Integración	La solución deberá permitir mecanismos seguros de integración y segmentación entre componentes de la arquitectura, conforme a las políticas de seguridad institucional.
39	Integración	La solución deberá contar con la capacidad de integrarse con plataformas SIEM y sistemas de gestión de registros.
40	Integración	La solución deberá contar con la capacidad de integrarse con las herramientas de seguridad existentes en la Universidad Distrital, incluyendo el firewall de Palo Alto Networks (NGFW 3420), el EDR de Kaspersky y la plataforma de monitoreo y gestión de eventos SolarWinds Security Event Manager (SEM).

Ítem	Característica técnica	Descripción
41	Monitoreo, Reportes y Analítica de la plataforma	La solución deberá proporcionar capacidades de análisis automatizado y generación de alertas en tiempos acordes con la operación y monitoreo continuo de la infraestructura institucional.
42	Monitoreo, Reportes y Analítica de la plataforma	La solución debe ser capaz de informar en tiempo real sobre el ancho de banda monitorizado, el estado de la interfaz de red y el estado de procesamiento de los tipos de tráfico de red.
43	Monitoreo, Reportes y Analítica de la plataforma	La solución deberá permitir la generación de reportes personalizables basados en eventos, alertas, incidentes y demás información recopilada por la plataforma.
44	Monitoreo, Reportes y Analítica de la plataforma	La solución deberá permitir la configuración de notificaciones automáticas por correo electrónico ante la generación de alertas o eventos de seguridad, dirigidas a los administradores o responsables designados para la gestión y atención de incidentes.
45	Monitoreo, Reportes y Analítica de la plataforma	La solución deberá proporcionar capacidades de analítica, visualización y correlación de eventos orientadas a la identificación de amenazas internas y externas sobre la infraestructura monitoreada.
46	Monitoreo, Reportes y Analítica de la plataforma	La solución debe tener la capacidad de crear informes ejecutivos diarios, semanales y mensuales y permitir la exportación de informes.
47	Monitoreo, Reportes y Analítica de la plataforma	La solución deberá proporcionar paneles y tableros personalizables para la visualización y análisis de información operativa y de seguridad, incluyendo como mínimo eventos registrados, estado del sistema, actividad de red, indicadores de compromiso, activos involucrados, alertas generadas y resultados analíticos obtenidos por la plataforma.
48	Visibilidad Extendida e Integración de la Solución NDR	La solución deberá permitir ampliar las capacidades de visibilidad y correlación sobre endpoints estratégicos, mediante agentes, sensores ligeros, telemetría de red u otros mecanismos soportados por el fabricante, con el fin de complementar la recolección de información de seguridad en escenarios donde el monitoreo basado únicamente en tráfico no sea suficiente (por ejemplo, usuarios remotos, tráfico cifrado o segmentos no instrumentados). La gestión y visualización de la información recolectada deberá realizarse desde una consola centralizada que permita capacidades de monitoreo, análisis, detección y respuesta desde una única interfaz.
49	Visibilidad Extendida e Integración de la Solución NDR	Los mecanismos de visibilidad utilizados sobre los equipos de cómputo deberán incluir como mínimo las siguientes capacidades: • Recolección de telemetría y contexto de seguridad. • Bajo impacto sobre el rendimiento de los dispositivos monitoreados. • Posibilidad de despliegue o habilitación selectiva sobre hasta cuatrocientos (400) equipos definidos por la Universidad. • Integración con la plataforma central de análisis para el envío de información y correlación de eventos.
50	Visibilidad Extendida e Integración de la Solución NDR	Los mecanismos utilizados para la recolección de telemetría y visibilidad sobre los endpoints no deberán interferir ni generar conflictos con las soluciones de seguridad existentes en la infraestructura institucional, incluyendo antivirus, EDR u otras herramientas de protección de endpoints, garantizando la convivencia operativa sobre los equipos monitoreados.
51	Visibilidad Extendida e Integración de la Solución NDR	La solución debe permitir la creación, ajuste e importación de reglas de detección basadas en el análisis de tráfico de red, comportamiento y anomalías, utilizando formatos estructurados y estandarizados de uso común en la industria, facilitando la interoperabilidad, reutilización y adaptación de reglas de detección existentes.
52	Visibilidad Extendida e Integración de la Solución NDR	La solución deberá permitir el análisis de archivos u objetos identificados dentro del tráfico de red mediante sandboxing, análisis dinámico u otros mecanismos equivalentes soportados por el fabricante permitiendo su inspección en entornos controlados para la detección de comportamientos maliciosos. Esta función debe permitir:

Ítem	Característica técnica	Descripción
		• Identificación de archivos u objetos sospechosos a partir del análisis del tráfico de red. • Envío automatizado de dichos objetos al entorno de sandbox para su análisis. • Integración con mecanismos o motores de análisis avanzado para la detección de amenazas desconocidas. • Generación de alertas y enriquecimiento de eventos a partir de los resultados del análisis avanzado realizado
53	Visibilidad Extendida e Integración de la Solución NDR	Los mecanismos de visibilidad utilizados sobre los endpoints deberán permitir la recolección de telemetría y contexto de seguridad desde los equipos monitoreados, con el fin de complementar las capacidades de visibilidad y correlación de la solución NDR.
54	Visibilidad Extendida e Integración de la Solución NDR	La solución deberá proporcionar visibilidad sobre la propagación y relación de amenazas dentro de la infraestructura monitoreada, incluyendo correlación entre eventos de red, activos involucrados y endpoints donde se desplieguen mecanismos de visibilidad extendida.
55	Visibilidad Extendida e Integración de la Solución NDR	La solución deberá permitir la integración con fuentes externas de telemetría, con el fin de enriquecer la base de datos de eventos y permitir su consulta desde la consola de análisis.
56	Visibilidad Extendida e Integración de la Solución NDR	La solución deberá permitir la búsqueda, consulta y correlación de indicadores de compromiso (IOC) sobre la telemetría centralizada recolectada, incluyendo información proveniente del tráfico de red y de los mecanismos de visibilidad extendida.
57	Visibilidad Extendida e Integración de la Solución NDR	La solución debe proporcionar una interfaz de búsqueda con funcionalidad avanzada que permita a los analistas realizar consultas sobre la telemetría y eventos recolectados.
58	Visibilidad Extendida e Integración de la Solución NDR	La solución debe ser capaz de detectar comunicaciones sospechosas dentro del tráfico de red monitoreado, incluyendo conexiones hacia infraestructuras de comando y control (C&C).
59	Visibilidad Extendida e Integración de la Solución NDR	Las alertas generadas deben enriquecerse automáticamente con información contextual relevante como descripciones, clasificación de amenazas y otros datos que faciliten el análisis.
60	Visibilidad Extendida e Integración de la Solución NDR	La solución deberá permitir el etiquetado de activos, equipos o segmentos de red, con el fin de facilitar la gestión y el análisis diferenciado.
61	Visibilidad Extendida e Integración de la Solución NDR	Las alertas y eventos generados deberán mapearse, cuando aplique, a tácticas, técnicas y procedimientos (TTP) de la matriz MITRE ATT&CK.
62	Visibilidad Extendida e Integración de la Solución NDR	La solución deberá permitir la gestión e incorporación de indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA), aplicables a los motores de análisis de red, sandbox y a las integraciones con otras herramientas de seguridad.
63	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución propuesta debe contar con capacidades avanzadas de detección de amenazas, incluyendo la capacidad de identificar y alertar en: • Ataques Zero-Day: vulnerabilidades previamente desconocidas o no parcheadas. • Amenazas Persistentes Avanzadas (APT): ataques sofisticados y dirigidos por grupos estatales u organizados. • Amenazas sofisticadas de red: incluyendo, pero no limitándose a, malware, ransomware y otros tipos de actividades maliciosas que evaden los controles de seguridad tradicionales.
64	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá contar con capacidades para la detección de malware avanzado, amenazas desconocidas y ataques de tipo zero-day, mediante técnicas de análisis avanzadas que permitan su identificación en tiempo cercano a real, incluso cuando no existan firmas previamente conocidas.
65	Capacidades Avanzadas de Detección, Análisis de	La solución deberá permitir capacidades de análisis dinámico o sandboxing sobre artefactos sospechosos identificados en el tráfico de red, utilizando entornos controlados

Ítem	Característica técnica	Descripción
	Amenazas y Comportamiento	compatibles con uno o varios sistemas operativos, ya sea de forma nativa o mediante integraciones soportadas por el fabricante.
66	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá permitir la recopilación y análisis de telemetría proveniente de sensores, agentes o mecanismos equivalentes, proporcionando información contextual sobre comportamientos sospechosos, indicadores de compromiso y posibles amenazas detectadas.
67	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá permitir la integración con agentes de endpoint, EDR u otros mecanismos equivalentes para el envío y análisis de archivos u objetos sospechosos mediante capacidades de análisis avanzado o sandboxing, ya sea de forma nativa o mediante integraciones soportadas por el fabricante.
68	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá proporcionar resultados detallados del análisis avanzado de amenazas o sandboxing, incluyendo información relacionada con procesos, comunicaciones de red, consultas DNS, comportamiento observado y demás indicadores relevantes que permitan a los analistas comprender las características y el impacto potencial de las amenazas detectadas.
69	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá permitir que las capacidades de análisis avanzado o sandboxing puedan ser utilizadas por múltiples nodos, centros de análisis o componentes de la arquitectura, conforme al diseño propuesto por el fabricante.
70	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá permitir, cuando aplique, capacidades controladas y configurables de comunicación externa para enriquecer el análisis avanzado de amenazas, incluyendo la validación de comportamientos, reputación o descarga de componentes requeridos para el análisis.
71	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá permitir técnicas avanzadas de análisis dinámico orientadas a identificar comportamientos maliciosos asociados a ejecución controlada, interacción simulada o activación de comportamientos sospechosos durante el análisis de amenazas.
72	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución debe ser capaz de procesar y analizar archivos, incluidos archivos protegidos por contraseña y documentos de oficina, independientemente de su origen
73	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá incorporar mecanismos orientados a mejorar la efectividad del análisis dinámico frente a amenazas que intenten detectar o evadir entornos de análisis automatizado.
74	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá proporcionar capacidades de análisis avanzado sobre objetos identificados en el tráfico de red, permitiendo obtener información relevante sobre su comportamiento, comunicaciones y posibles indicadores de compromiso.
75	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá permitir escalabilidad en las capacidades de análisis avanzado mediante mecanismos distribuidos o múltiples instancias de procesamiento, orientados a optimizar los tiempos de análisis y respuesta.
76	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	Los resultados obtenidos mediante las capacidades de análisis avanzado deberán poder enriquecer los procesos de correlación, reputación o detección utilizados por otras herramientas de seguridad integradas dentro de la infraestructura institucional.
77	Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento	La solución deberá permitir que múltiples componentes o nodos de análisis puedan utilizar capacidades centralizadas o compartidas de análisis avanzado de amenazas, conforme a la arquitectura propuesta por el fabricante.

Ítem	Característica técnica	Descripción
78	Capacidades NDR	La solución deberá proporcionar capacidades de análisis y visibilidad del tráfico de red, permitiendo como mínimo: • Visualización e inspección de eventos de tráfico de red en tiempo real. • Análisis de capturas de paquetes y/o flujos de red. • Identificación de amenazas, anomalías y comportamientos sospechosos en el tráfico monitoreado. • Soporte a procesos de investigación y respuesta ante incidentes de seguridad.
79	Capacidades NDR	La solución deberá proporcionar recomendaciones de investigación, contención o remediación ante alertas de seguridad generadas por la plataforma, con el fin de apoyar a los administradores en la investigación y remediación de incidentes.
80	Capacidades NDR	La solución debe ser capaz de recibir entradas para indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA) para clasificar y analizar eventos.
81	Capacidades NDR	La solución debe permitir la creación e importación de reglas de detección de red utilizando formatos abiertos y estandarizados de uso común en la industria.
82	Capacidades NDR	La solución deberá permitir habilitar, deshabilitar, ajustar o excluir reglas de detección de red, conforme a las necesidades operativas de la Universidad.
83	Capacidades NDR	La solución deberá permitir la exportación en formato PCAP del tráfico de red asociado a eventos detectados, con fines de análisis forense.
84	Capacidades NDR	La solución deberá soportar despliegues en modo de monitorización mediante SPAN, port mirroring o mecanismos equivalentes.
85	Capacidades NDR	La solución debe poder funcionar en modo de monitorización (fuera de banda), sin interferir con la comunicación entrante/saliente ni interrumpir los procesos empresariales.
86	Capacidades NDR	La solución deberá permitir el reanálisis de eventos, objetos o tráfico previamente almacenado utilizando inteligencia de amenazas, reglas o capacidades analíticas actualizadas, con el fin de identificar amenazas no detectadas inicialmente.
87	Capacidades NDR	La solución deberá permitir la integración con mecanismos de respuesta o contención sobre endpoints, firewalls u otras herramientas de seguridad, posibilitando acciones automatizadas o asistidas ante amenazas detectadas.
88	Capacidades NDR	Las acciones sospechosas detectadas deben relacionarse con fases de ataque, técnicas de hackers y métodos de la matriz MITRE ATT&CK.
89	Capacidades NDR	La solución debe tener la capacidad de importar y/o personalizar reglas que permitan complementar las predeterminadas y extiendan su uso en el escaneo de objetos del tráfico de red, archivos, objetos e inspección profunda del tráfico, detección de infraestructuras c2c conocidas y reputación de dominios.
90	Capacidades NDR	La solución deberá permitir la identificación de infraestructuras de comando y control (C2), incluyendo aquellas previamente desconocidas, mediante mecanismos de análisis, detección e inteligencia de amenazas actualizada proporcionada por el fabricante o fuentes integradas compatibles.
91	Capacidades NDR	La solución deberá ser capaz de analizar y detectar en el tráfico los objetos que puedan contener patrones con técnicas como evasión, trafico malicioso asociado a comunicaciones de comando y control (C2).
92	Capacidades NDR	La solución proporcionará un inventario lógico de activos monitoreados, incluyendo: • Información de la cuenta de usuario registrada en los sistemas operativos del dispositivo. • Información relacionada con actividad o ejecución de archivos, cuando dicha visibilidad se encuentre disponible mediante las capacidades ofertadas. • Espacios de direcciones de dispositivos (por ejemplo, direcciones IP, direcciones MAC).
93	Capacidades NDR	La solución permitirá mostrar los riesgos asociados a los dispositivos, facilitando la gestión proactiva de amenazas.
94	Capacidades NDR	Para proporcionar una visibilidad completa de la actividad del endpoint, la solución deberá integrarse con los agentes endpoint protegidos por la solución EDR institucional

Ítem	Característica técnica	Descripción
		desde los que enviar datos adicionales de telemetría de red, proporcionando contexto complementario, incluyendo, pero no limitado a: • Nombres de procesos del sistema que inician conexiones de red. • Ruta del sistema de archivos al proceso del sistema que inicia la conexión de red.
95	Capacidades NDR	La solución debe proporcionar capacidades de respuesta de red, incluida la integración con dispositivos de comunicación de red, para permitir acciones de aislamiento, contención o respuesta asistida o automatizada del host. La solución también facilitará la recopilación de información adicional sobre los activos de la red para apoyar la respuesta a incidentes y la mitigación de amenazas.
96	Capacidades NDR	La solución debe soportar direccionamiento IP dinámico de los dispositivos, asegurando un seguimiento y monitorización precisos.
97	Capacidades NDR	La solución proporcionará monitorización en tiempo real de la actividad de red de los dispositivos mediante capacidades gráficas o visuales de representación de actividad y relaciones de red, permitiendo la visualización del tráfico de red y posibles amenazas de seguridad.
98	Capacidades NDR	La solución permitirá un sondeo activo y configurable de dispositivos para enriquecer la información del dispositivo y construir un mapa topológico de red completo.
99	Capacidades NDR	La solución debe permitir el análisis de tráfico cifrado mediante técnicas de fingerprinting TLS u otros métodos equivalentes que faciliten la detección de comportamientos anómalos sin requerir descifrado del contenido.
100	Capacidades NDR	A efectos de la investigación forense, respuesta a incidentes o cumplimiento normativo de incidentes cibernéticos, la solución debe proporcionar la capacidad de capturar y registrar el tráfico de red en bruto.
101	Capacidades NDR	El tráfico grabado puede capturarse en un formato que puede analizarse y reproducirse fácilmente, como PCAP (Captura de Paquetes).
102	Capacidades NDR	La solución debe proporcionar una interfaz de descarga para el tráfico grabado que soporte capacidades de filtrado usando la sintaxis BPF y expresiones regulares. Esta interfaz permitirá a los usuarios recuperar y analizar de forma eficiente subconjuntos específicos del tráfico registrado, facilitando una mejor respuesta a incidentes, la búsqueda de amenazas y la monitorización de la seguridad.
103	Capacidades NDR	La solución NDR deberá realizar inspección profunda de tráfico (Deep Packet Inspection – DPI), permitiendo identificar y analizar protocolos comunes y propietarios, sin limitarse a una lista cerrada de protocolos predefinidos.
104	Capacidades NDR	La solución permitirá la búsqueda y recuperación de sesiones de red basándose en capturas de paquetes en el almacenamiento de tráfico.
105	Capacidades NDR	La solución permitirá la exportación de tráfico de red para su análisis posterior, mediante paquetes, datos de sesión o una combinación de ambos

Tabla 1. Requerimientos técnicos mínimos obligatorios

5. Certificaciones técnicas solicitadas

Las certificaciones solicitadas son las siguientes y deberán estar vigentes a la fecha de presentación de la oferta:

a. El fabricante de la solución ofrecida deberá haber sido reconocido dentro de los últimos tres (3) años en informes de analistas de la industria tales como Gartner Magic Quadrant, The Forrester Wave™, ISG Provider Lens™, SPARK Matrix™ (QKS Group), Radicati Market Quadrant u otros estudios equivalentes de firmas internacionales de análisis del mercado, en categorías relacionadas

Endpoint Protection Platforms (EPP), Network Detection and Response (NDR), Extended Detection and Response (XDR) o Threat Intelligence.

b. Los componentes de la solución no deberán encontrarse en estado de End of Sale (EOS) ni End of Life (EOL) al momento de la presentación de la oferta. El fabricante deberá garantizar un ciclo de vida y soporte no inferior a cinco (5) años, incluyendo actualizaciones de seguridad y soporte técnico.

c. Certificación vigente expedida por el fabricante que acredite la condición del oferente como canal autorizado o partner oficial para la comercialización, implementación y soporte de la solución ofertada, en un nivel superior dentro del esquema de certificación del fabricante.

Nota: En el caso de proponentes plurales, estos requisitos deberán ser cumplidos por al menos uno de los integrantes que tenga relación directa con el fabricante de la solución ofertada y que respalde la totalidad de la solución propuesta, incluyendo licenciamiento, componentes físicos y servicios asociados.

6. Proceso de implementación

Previo al inicio de las actividades de implementación, el contratista deberá presentar para aprobación de la supervisión un cronograma de implementación de la solución y un plan de pruebas de funcionamiento, en los cuales se definan las actividades, tiempos, responsables y validaciones técnicas asociadas al despliegue de la solución. La implementación de la solución deberá garantizar los siguientes aspectos:

a. **Instalación del hardware:** instalación y puesta en funcionamiento de todos los componentes físicos de la solución sobre la infraestructura tecnológica, así como el licenciamiento asociado a la solución de detección, prevención y respuesta ante ciberamenazas a nivel de red, suministrados por el contratista y aprobados por la Universidad.

b. **Instalación y configuración de software:** Instalación, activación y configuración del software asociado a la solución de detección, prevención y respuesta ante ciberamenazas a nivel de red, incluyendo la plataforma central de administración y análisis, componentes de monitoreo, módulos analíticos, licenciamiento y demás elementos lógicos requeridos para la operación de la solución ofertada bajo arquitectura On-Premise.

Activación, despliegue y configuración de las capacidades de visibilidad, monitoreo y correlación de eventos para los cuatrocientos (400) endpoints definidos por la Universidad, garantizando la correcta integración y envío de telemetría, eventos de seguridad y metadatos hacia la consola central de administración y análisis implementada. El licenciamiento deberá iniciar cuando esta prueba sea exitosa.

c. **Configuración de políticas:** El contratista deberá realizar la configuración y ajuste inicial de políticas, reglas de detección, monitoreo, alertamiento y correlación de eventos de la solución, de acuerdo con los requerimientos técnicos y lineamientos de seguridad definidos por la Universidad.

d. **Integración:** El contratista deberá realizar la configuración e integración de la solución con las herramientas de seguridad y monitoreo existentes en la Universidad Distrital, incluyendo Firewall Palo Alto Networks, EDR Kaspersky y SolarWinds, con el fin de fortalecer las capacidades de correlación de eventos, monitoreo centralizado y respuesta ante incidentes de seguridad.

e. Pruebas de funcionamiento:

i. **Validación de captura y análisis de tráfico de red**: Comprobación de la correcta recepción y análisis del tráfico de red proveniente de los puntos de monitoreo definidos (Core, DMZ y Data Center institucionales), mediante la verificación de flujos de tráfico, generación de eventos de seguridad y visualización en la consola de administración.

ii. **Prueba de detección de eventos de seguridad**: Realización de pruebas controladas que permitan validar la capacidad de la solución para detectar comportamientos anómalos o eventos de seguridad en el tráfico de red, generando las respectivas alertas en la plataforma.

iii. **Validación de integraciones**: Verificación de la correcta integración de la solución con las plataformas institucionales de seguridad y monitoreo, incluyendo la interacción con el Firewall Palo Alto, el EDR Kaspersky y la herramienta de monitoreo SolarWinds, de acuerdo con las capacidades definidas en el alcance del contrato.

iv. **Prueba de simulación de ataque controlado:** Se deberán realizar pruebas controladas de simulación de amenazas con el fin de validar la capacidad de la solución para identificar comportamientos maliciosos dentro de la red institucional. Estas pruebas podrán incluir actividades como generación de tráfico sospechoso, intentos de escaneo de red, comunicación con dominios o direcciones IP simuladas como maliciosas o catalogadas como sospechosas, así como otros escenarios definidos de manera conjunta entre el contratista y la Universidad. La solución deberá generar las alertas correspondientes en la consola de administración y evidenciar las capacidades de análisis, correlación y visibilidad del evento detectado.

v. **Prueba de operación:** Verificación de la correcta operación de la solución una vez finalizado el proceso de instalación, validando el funcionamiento conjunto de los componentes de la plataforma, la generación de alertas y la visualización de eventos en la consola de administración.

f. Entrega de documentación técnica: El contratista deberá entregar un informe técnico que incluya como mínimo:

i. Arquitectura implementada de la solución.
ii. Componentes y/o licenciamientos instalados y configuraciones principales.
iii. Resultados de las pruebas realizadas.
iv. Evidencias de funcionamiento de la plataforma.
v. Recomendaciones técnicas para la operación y administración de la solución.

g. Transferencia de conocimiento: El contratista deberá realizar jornadas de capacitación técnica y transferencia de conocimiento dirigidas al personal designado por la supervisión, orientadas a la administración, monitoreo y operación de la solución implementada, con una duración mínima de doce (12) horas y entregar la documentación técnica y material de apoyo.

h. Periodo de estabilización de la plataforma: Una vez finalizado el proceso de implementación y puesta en funcionamiento de la solución, se deberá contemplar un periodo de estabilización entre treinta (30) y noventa (90) días calendario, durante el cual el contratista realizará los ajustes y afinamientos necesarios en configuraciones, reglas de detección e integraciones, con el fin de optimizar el desempeño de la plataforma y reducir la generación de falsos positivos. Estas actividades se realizarán en coordinación con el personal técnico designado por la Universidad.

7. Garantía técnica

El contratista deberá garantizar el correcto funcionamiento de la solución de detección, prevención y respuesta ante ciberamenazas a nivel de red durante la vigencia del licenciamiento, asegurando la operación continua de todos los componentes suministrados.

Las condiciones mínimas de la garantía técnica serán las siguientes:

i. **Tiempo de cobertura**: La solución deberá contar con garantía técnica mínimo de un (1) año, contado a partir de la puesta en correcto funcionamiento de la plataforma y la firma del acta de recibo a satisfacción.

ii. **Alcance de la garantía:** La garantía cubrirá defectos de funcionamiento, errores asociados a la implementación de la solución y fallas en los componentes de software suministrados, así como en los componentes físicos, appliances, sensores, colectores, licenciamiento y demás elementos que hagan parte de la solución, asegurando su corrección sin costo adicional para la entidad.

El contratista deberá garantizar la reposición o sustitución de componentes físicos defectuosos (hardware), cuando la falla sea atribuible a defectos de fabricación, configuración o funcionamiento de la solución suministrada.

Si el proceso de garantía requiere algún equipo se retire de las instalaciones de la Universidad, este deberá ser reemplazado por uno de iguales o superiores características para no afectar el servicio.

En caso de ser necesario el traslado del equipo o sus componentes, el desplazamiento (ida y vuelta), los costos asociados a este desplazamiento (fletes, seguros, etc.) y la responsabilidad por el equipo están a cargo exclusivo del contratista. Las labores realizadas deben generar informes escritos que incluyen entre otros:

- El diagnóstico y concepto técnico sobre la falla.
- Listado de seriales y denominación de partes reemplazadas y retiradas
- Causas que generaron la falla.

iii. **Restablecimiento del servicio**: En caso de presentarse fallas en la operación de la solución, se deberá brindar acompañamiento técnico hasta lograr el restablecimiento del servicio y la correcta operación de la plataforma.

8. Soporte de fábrica

El fabricante deberá garantizar que la solución cuente con soporte de fabrica durante toda la vigencia del licenciamiento. Las condiciones mínimas del soporte de fábrica serán las siguientes:

a. **Cobertura del soporte**: El servicio de soporte técnico proveniente por el fabricante, deberá prestarse en esquema 7x24 (siete días de la semana, veinticuatro horas al día), en un tiempo no

superior a 4 horas, para la atención de incidentes o fallas relacionadas con la operación de la solución.

b. Soporte técnico especializado- nivel 2 y/o superior: El fabricante deberá disponer de personal técnico especializado en la solución implementada, con capacidad para brindar atención y acompañamiento para la resolución de incidentes, fallas de funcionamiento, problemas de integración o requerimientos técnicos asociados con la plataforma. La atención de soporte de fabrica podrá realizarse mediante los siguientes canales:

- Atención remota a través de sistema de tickets o correo electrónico.

c. Base de conocimiento y escalamiento: Acceso a portales oficiales, documentación técnica y escalamiento de casos a niveles avanzados del fabricante cuando sea requerido.

9. Soporte de Partner

El contratista deberá garantizar que la solución cuente con soporte durante toda la vigencia del licenciamiento. Las condiciones mínimas del soporte de partner serán las siguientes:

a. Cobertura del soporte: El servicio de soporte técnico proveniente por el partner, deberá prestarse en esquema 7x24 (siete días de la semana, veinticuatro horas al día), en un tiempo no superior a 4 horas para la atención de incidentes o fallas relacionadas con la operación de la solución (hardware y licenciamiento de la solución).

b. Soporte técnico especializado de primer nivel: El contratista deberá disponer de personal técnico especializado en la solución implementada, con capacidad para brindar atención y acompañamiento para la resolución de incidentes, fallas de funcionamiento, problemas de integración o requerimientos técnicos asociados con la plataforma de primer nivel. La atención de soporte podrá realizarse mediante los siguientes canales:

- Atención remota a través de sistema de tickets o correo electrónico.
- Atención telefónica para incidentes críticos.
- Atención en sitio cuando la naturaleza del incidente lo requiera y no pueda ser resuelto de forma remota.

c. Mantenimiento y Actualizaciones del software: Durante el periodo de garantía técnica el contratista deberá garantizar el acceso y aplicación de actualizaciones de la plataforma, incluyendo:

- **Updates:** actualizaciones menores orientadas a corrección de errores, parches de seguridad, mejoras de estabilidad y actualización de firmas o motores de detección.
- **Upgrades:** actualizaciones mayores que impliquen cambio de versión o incorporación de nuevas funcionalidades del producto.

Como mínimo, se deberán realizar dos (2) mantenimientos preventivos sobre los componentes de software de la solución, durante el periodo de licenciamiento.

d. Mantenimiento preventivos Hardware: Se entiende por mantenimiento preventivo: Las estrategias que pretenden maximizar la vida útil y operativa de las máquinas y sus componentes, identificando las posibles causas que pueden originar fallas futuras e indicando las medidas a

tomar para evitar dichas fallas, así como Las actividades conducentes a detectar y evitar fallas antes que sucedan, para dar tiempo de corregirlas sin perjuicios a la funcionalidad y servicio continuo que presta el hardware de la solución

i. Condiciones

- Se realizará un mantenimiento preventivo a los seis (6) meses después de la puesta en correcto funcionamiento.
- El manejo de los equipos se debe realizar de acuerdo a los procedimientos indicados por el fabricante para apagado, encendido y demás acciones que se realicen. Los manuales o protocolos de mantenimiento, deben ser entregados previos a la intervención de los equipos.
- A partir del momento en que se permita acceso al lugar de localización de los equipos, en donde se realizará la rutina de mantenimiento, el contratista se hace responsable completamente por la integridad física y lógica de los mismos, así como de la integridad de los datos almacenados, la integridad y normal funcionamiento e interconexión de los elementos y hardware de la solución y los equipos o componentes que se encuentren en el Data Center.

ii. Procedimiento de mantenimiento preventivo

Debe incluir como mínimo las siguientes actividades:

- Revisión de las condiciones iniciales de funcionamiento del equipo, componente y aplicaciones alojadas, a través de lista de chequeo suministrada por el administrador del sistema y del equipo.
- Antes de cualquier procedimiento de soporte o mantenimiento se deben realizar los backup correspondientes a la solución
- Realizar actualizaciones del firmware, que sean requeridas y aprobadas, en los equipos de la solución
- Después del mantenimiento se realizará pruebas de funcionamiento del equipo.
- Pruebas de conectividad en red, de interconexión con los elementos que lo conforman y su correcto funcionamiento.
- Pruebas de correcto funcionamiento de la solución avalada por el administrador
- El contratista debe entregar Informe Técnico en forma escrita y en medio magnético y debe incluir como mínimo
  - ✓ Registro de eventos y fallas.
  - ✓ Análisis técnico e interpretación del registro de eventos presentes

10. Glosario

- **7x24:** Servicio de soporte disponible las 24 horas del día, los 7 días de la semana, que incluye atención de incidentes y, de ser necesario, reemplazo de hardware al siguiente día hábil.
- **Actualización (Update):** Correcciones menores, parches de seguridad o mejoras funcionales aplicadas a una solución tecnológica sin implicar un cambio de versión principal.

- **Actualización mayor (Upgrade):** Cambio de versión de un sistema o software que incorpora mejoras significativas, nuevas funcionalidades o modificaciones estructurales.
- **Alta disponibilidad (HA):** Configuración tecnológica que permite mantener la operación continua de un sistema o servicio ante fallas de alguno de sus componentes, mediante mecanismos de redundancia y conmutación automática.
- **APT (Advanced Persistent Threat):** Amenaza avanzada y persistente caracterizada por ataques dirigidos, sofisticados y prolongados en el tiempo, cuyo objetivo es comprometer sistemas o información crítica de una organización.
- **Backdoor:** Tipo de malware diseñado para permitir el acceso remoto no autorizado a un sistema informático, otorgando control a un atacante sin el conocimiento del usuario.
- **EDR (Endpoint Detection and Response):** Solución de seguridad instalada en los equipos finales (endpoints) que permite detectar, analizar y responder a amenazas avanzadas mediante monitoreo continuo, análisis de comportamiento y capacidades de contención y remediación.
- **Endpoint:** Dispositivo o equipo final, como computadores de escritorio o portátiles, en el cual se instalan herramientas o soluciones de seguridad para su protección.
- **Exploits:** Programa o código que aprovecha una vulnerabilidad o fallo de seguridad en una aplicación, sistema o software con el fin de ejecutar acciones maliciosas o no autorizadas.
- **Firewall:** Dispositivo o sistema de seguridad que controla y filtra el tráfico de red entrante y saliente con base en políticas previamente definidas, permitiendo la protección perimetral y la segmentación de la red.
- **Integración:** Capacidad de una plataforma tecnológica para intercambiar información y eventos con otras soluciones de seguridad o sistemas existentes (EDR, SIEM, firewall, entre otros).
- **Keyloggers:** Tipo de software malicioso que registra cada tecla pulsada en un dispositivo, generalmente sin el conocimiento del usuario, con el fin de capturar información sensible como contraseñas o datos personales.
- **NDR (Network Detection and Response):** Plataforma de detección y respuesta a nivel de red que analiza el tráfico interno y externo para identificar comportamientos anómalos, amenazas avanzadas, movimientos laterales y ataques dirigidos.
- **Phishing:** Técnica de ingeniería social utilizada por ciberdelincuentes para obtener información confidencial, como credenciales de acceso o datos personales, mediante el envío de correos electrónicos o mensajes fraudulentos que suplantan entidades legítimas.
- **Rootkits:** Conjunto de herramientas de software malicioso diseñadas para permitir acceso no autorizado a un sistema y ocultar la presencia de otros programas maliciosos.
- **Sandboxing:** Tecnología que permite ejecutar archivos o código sospechoso en un entorno aislado y controlado con el fin de analizar su comportamiento sin afectar la infraestructura productiva.
- **SIEM (Security Information and Event Management):** Plataforma que recopila, correlaciona y analiza eventos y registros de seguridad provenientes de múltiples fuentes (firewalls, servidores, endpoints, aplicaciones), generando alertas y reportes para la gestión de incidentes.
- **Spyware:** Software malicioso diseñado para recopilar información de un dispositivo y enviarla a un tercero sin el conocimiento ni consentimiento del usuario.
- **Troyanos:** Tipo de software malicioso que se presenta como un programa legítimo y que, una vez instalado, permite la instalación de otros programas o malware sin el consentimiento del usuario.