UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

ESPECIFICACIONES TÉCNICAS
UNIDAD RED DE DATOS UDNET

Contenido

Especificaciones técnicas

1. Objeto del proceso

Adquirir el licenciamiento de una plataforma de detección, prevención y respuesta ante ciberamenazas a nivel de red, incluyendo su instalación, configuración y puesta en funcionamiento en la infraestructura tecnológica de la Universidad Distrital Francisco José de Caldas, con el fin de fortalecer las capacidades de seguridad informática y garantizar la continuidad de los servicios tecnológicos institucionales, así como la prestación de soporte técnico especializado en modalidad 7x24.

2. Alcance técnico

El alcance del proyecto incluye la adquisición del licenciamiento, implementación, integración y puesta en operación de una plataforma de detección, prevención y respuesta ante ciberamenazas a nivel de red, orientada a fortalecer las capacidades de seguridad informática de la Universidad Distrital Francisco José de Caldas. En este proceso se busca dar solución a los siguientes ítems:

a. Suministro de licenciamiento: Licenciamiento de una solución de detección, prevención y respuesta a nivel de red por un periodo mínimo de un (1) año, incluyendo el derecho a actualizaciones (updates y upgrades) durante la vigencia del licenciamiento, así como los servicios necesarios para su activación, instalación y configuración inicial.

Adicionalmente, se requiere el licenciamiento correspondiente para la protección de cuatrocientos (400) endpoints, por un periodo mínimo de un (1) año, como complemento a la solución de detección, prevención y respuesta de red e implementación inicial orientada a fortalecer las capacidades de monitoreo, detección y respuesta ante incidentes de seguridad en equipos estratégicos de la entidad.

b. Implementación: Instalación, configuración y puesta en correcto funcionamiento de la solución, incluyendo el despliegue de sensores o colectores de tráfico en puntos estratégicos de la infraestructura institucional (Core, DMZ, Data Center Sabio Caldas y sede Bosa Porvenir), utilizando la infraestructura de servidores que será suministrada por la Universidad Distrital.

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, validación de captura de tráfico y verificación de detección de eventos de seguridad, que permitan

evidenciar la correcta operación de la solución previo al recibo a satisfacción por parte de la supervisión.

c. 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.

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

Adicionalmente, 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.

e. **Transferencia de conocimiento:** Realización de actividades de capacitación técnica y transferencia de conocimiento dirigidas al personal designado por la Universidad, orientadas a la administración, monitoreo y operación de la solución implementada.

   La capacitación deberá contemplar un mínimo de doce (12) horas, y deberá incluir, como mínimo, aspectos relacionados con la arquitectura de la solución, administración de la plataforma, análisis de alertas, procedimientos básicos de respuesta a incidentes y buenas prácticas de operación. El contratista deberá suministrar la documentación técnica y el material de apoyo correspondiente.

Nota 1: La infraestructura física en la cual se realizará la instalación de la plataforma será proporcionada por la Universidad Distrital Francisco José de Caldas mediante un proceso de adquisición independiente. En consecuencia, los servidores requeridos para la instalación y operación de la solución no deberán ser incluidos ni considerados dentro del alcance ni de la oferta del presente proceso de contratación. Las características técnicas de la adquisición de los servidores se encuentran en el Anexo 1 del presente documento.

Nota 2: Se deberá tener en cuenta que la disponibilidad de los servidores mencionados depende de la culminación del proceso de adquisición correspondiente el cual se llevará a cabo en paralelo con el presente proceso de contratación; por lo tanto, las actividades de instalación e implementación de la solución deberán programarse y coordinarse de acuerdo con la disponibilidad de dicha infraestructura. En este sentido, sin estos servidores en las instalaciones de la Universidad no será posible iniciar el proceso de instalación y configuración de la plataforma.

Nota 3: Previo al proceso de instalación, se deberá realizar una sesión técnica de alistamiento entre el contratista y el personal designado por la Universidad, con el fin de definir y validar las configuraciones requeridas en los servidores que soportarán la solución.

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, así como 30 licencias de Hybrid Cloud Security para servidores y 200 licencias para entornos de escritorio, instaladas 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 el año 2023 se incorporó la plataforma de detección, prevención y respuesta ante amenazas avanzadas Kaspersky Anti Targeted Attack Platform (KATA), junto con 200 licencias para Endpoints instaladas en equipos estratégicos, las cuales estuvieron en uso hasta el 27 de diciembre de 2024, fecha en la cual finalizó su operación. Dicha plataforma incorpora capacidades de análisis avanzado del tráfico de red, Sandboxing y correlación con Endpoints, permitiendo identificar comportamientos anómalos, amenazas persistentes avanzadas (APT) y ataques dirigidos.

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) licenciamiento actualmente contratado y activo. 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 del licenciamiento, soporte técnico especializado en esquema 7x24 y el derecho a actualizaciones (updates y upgrades) de una

plataforma de detección, prevención y respuesta ante ciberamenazas a nivel de red, que permita complementar las capacidades actuales de seguridad, mejorar la visibilidad del tráfico interno de la red y facilitar la integración con las herramientas de seguridad y monitoreo existentes en la Universidad.

Adicionalmente, con el fin de fortalecer las capacidades de detección y respuesta ante amenazas que puedan originarse directamente en los equipos finales o evadir los mecanismos de monitoreo de red, se requiere complementar la solución mediante el licenciamiento de agentes EDR-NDR para un conjunto de cuatrocientos (400) equipos estratégicos dentro de la infraestructura institucional.

Estos agentes permitirán ampliar la visibilidad sobre el comportamiento de los endpoints, mejorar la correlación de eventos entre red y equipos finales y fortalecer las capacidades de detección temprana y contención de amenazas avanzadas, debiendo ser compatibles e integrarse con la solución de protección de endpoints actualmente implementada en la Universidad Distrital basada en Kaspersky Endpoint Security (EDR).

4. Requerimientos técnicos mínimos obligatorios

La solución a adquirir deberá cumplir con los requerimientos técnicos mínimos orientados a asegurar capacidades avanzadas de monitoreo de tráfico, detección de amenazas, análisis de comportamiento, generación de alertas, respuesta ante incidentes, integración con la infraestructura tecnológica existente y soporte técnico especializado 7x24, incluyendo el derecho a actualizaciones (update y upgrade) durante la vigencia del contrato.

Ítem	Característica técnica	Descripción
1	Requisitos Generales	La solución deberá permitir configuraciones que garanticen que la información analizada permanezca bajo control de la entidad cuando se requiera, conforme a las políticas de seguridad institucional.
2	Requisitos Generales	La solución debe ser capaz de escalar para soportar el crecimiento progresivo de endpoints en la organización, garantizando procesamiento eficiente y arquitectura escalable conforme a las necesidades institucionales.
3	Requisitos Generales	La solución debe ser compatible y capaz de recopilar, procesar y analizar datos de telemetría de endpoints que ejecuten sistemas operativos Windows, Linux y MacOS.
4	Requisitos Generales	La solución debe conservar todos los datos de telemetría de red y puntos finales localmente, con configuraciones de almacenamiento configurables para adaptarse a necesidades específicas de retención y gestión de datos.
5	Requisitos Generales	La solución deberá contar con una plataforma de seguridad unificada que integre capacidades de detección y respuesta a nivel de red (NDR), detección y respuesta en endpoints (EDR) y análisis avanzado de amenazas mediante sandbox, permitiendo la interacción y correlación de eventos entre los diferentes componentes de seguridad con el fin de mejorar la visibilidad, detección y respuesta ante incidentes

Ítem	Característica técnica	Descripción
6	Requisitos Generales	La solución deberá permitir una arquitectura distribuida, soportando la instalación de al menos un (1) nodo central de administración y análisis principal en la sede Calle 40, y al menos un (1) sensor de red adicional en la sede Bosa. La administración, configuración de políticas, correlación de eventos y generación de reportes deberá realizarse desde una única consola centralizada. La comunicación entre sensores y el nodo central deberá realizarse de forma segura y cifrada.
7	Arquitectura y Diseño de la Plataforma	La solución debe contar con capacidades centralizadas de investigación que permitan analizar la telemetría de red y de los endpoints licenciados, incluyendo el análisis del tráfico de red asociado a protocolos de correo electrónico cuando estos sean visibles a nivel de red.
8	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.
9	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 (por ejemplo, hasta 4 Gbps o superior), sin degradación del análisis ni pérdida de visibilidad.
10	Arquitectura y Diseño de la Plataforma	La solución debe diseñarse para garantizar una alta disponibilidad para los Centros de Análisis, con características como: • Redundancia y capacidades de conmutación por error para minimizar el tiempo de inactividad. • Balanceo de carga para distribuir la carga de trabajo entre varios nodos. • Failover y recuperación automatizados para garantizar un funcionamiento continuo. • Esta arquitectura de alta disponibilidad debe garantizar que los Centros de Análisis sigan operativos y respondiendo, incluso en caso de fallos de hardware o software.
11	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.
12	Arquitectura y Diseño de la Plataforma	La solución debe soportar la instalación de entornos VMware ESXi y KVM
13	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.
14	Administración de la Plataforma	La solución debe contar con una gestión unificada de políticas, informes centralizados e interfaz de ejecución de tareas dentro de una sola consola para una gestión centralizada.
15	Administración de la Plataforma	La solución debe ser capaz de utilizar un servidor proxy con autenticación para descargar actualizaciones de software.
16	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 (global o por dominio/tenant). • 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.
17	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.

Ítem	Característica técnica	Descripción
18	Administración de la Plataforma	La solución debe soportar sincronización de tiempo con servidores NTP.
19	Administración de la Plataforma	La solución debe soportar copias de seguridad y restauración. La copia de seguridad debe contener al menos: alertas, bases de datos, listas blancas, notificaciones, etc.
20	Administración de la Plataforma	La actualización del servidor de administración no debe requerir instalación desde cero ni pérdida de configuraciones, base de datos de incidentes, etc.
21	Administración de la Plataforma	Las acciones de los usuarios del sistema deben registrarse tanto en el registro de actividad local como de forma remota.
22	Administración de la Plataforma	La solución debe soportar actualizaciones fluidas del Centro de Análisis, permitiendo preservar los entornos existentes, la base de datos de incidentes y otros datos críticos, sin requerir una reinstalación completa desde cero, minimizando así los tiempos de inactividad y garantizando la continuidad de las operaciones.
23	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.
24	Integración	El proveedor debe ofrecer una opción para instalar una versión local de los servicios de inteligencia de amenazas, permitiendo establecer reputación personalizada para hashes y URLs. Esta versión local debe ser capaz de recibir información de seguridad de la solución para compartirla entre controles de seguridad integrados, mejorando así la postura de seguridad corporativa.
25	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.
26	Integración	La solución debe proporcionar una API completa que soporte las siguientes funcionalidades: • 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.
27	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).
28	Integración	La solución debe soportar el envío de alertas de ciberseguridad y la monitorización de información mediante syslog.
29	Integración	Los datos de reputación en los servicios de Inteligencia de Amenazas in situe deben actualizarse automáticamente con la información analítica obtenida de la solución. Esto permite enriquecer datos de amenazas en todas las soluciones conectadas a réplicas locales de servicios de inteligencia de amenazas
30	Integración	La nube de Inteligencia de Amenazas Privada debe tener una opción para añadir o redefinir objetos y recursos web datos de reputación personalizados.
31	Integración	La solución deberá permitir esquemas de integración segura unidireccional en entornos que requieran segmentación estricta entre redes.
32	Integración	La solución deberá contar con la capacidad de integrarse con plataformas SIEM y sistemas de gestión de registros.
33	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).
34	Monitoreo, Reportes y Analítica de la plataforma	La solución debe proporcionar tiempos de análisis eficientes y acordes con estándares de mercado, proporcionando informes oportunos tras el envío del objeto al subsistema de análisis automatizado.

Ítem	Característica técnica	Descripción
35	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.
36	Monitoreo, Reportes y Analítica de la plataforma	La solución debe tener informes personalizables basados en la información de las alertas
37	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.
38	Monitoreo, Reportes y Analítica de la plataforma	La solución debe proporcionar capacidades analíticas y de visualización, y detectar o combatir amenazas internas y externas avanzadas.
39	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.
40	Monitoreo, Reportes y Analítica de la plataforma	La solución debe proporcionar un número de paneles personalizables para obtener información sobre la actividad del sistema y resultados analíticos, incluyendo, pero no limitándose a: estado y actividad del sistema, longitudes de colas, eventos registrados, su estado y las tecnologías utilizadas para emitir veredictos, listas de IPs, dominios y correos electrónicos más frecuentemente relacionados con incidentes
41	Monitoreo, Reportes y Analítica de la plataforma	La solución proporcionará varios tipos de informes, ofreciendo una mayor visibilidad sobre la actividad de la red, el inventario de dispositivos y los posibles riesgos de seguridad.
42	Arquitectura e Integración del Componente EDR	La solución propuesta de Detección y Respuesta de Endpoint (EDR) debe estar completamente integrada con la solución de Protección Avanzada contra Amenazas (ATP), lo que permite compartir sin interrupciones inteligencia de amenazas, datos de incidentes y acciones de respuesta entre ambos sistemas. La integración debe proporcionar las siguientes capacidades: • **Compartición bidireccional de datos:** Las soluciones EDR y ATP deben ser capaces de compartir datos de amenazas, información de incidentes y acciones de respuesta en tiempo real. • **Respuesta unificada a incidentes:** Las soluciones EDR y ATP deben proporcionar un flujo de trabajo unificado de respuesta a incidentes, permitiendo a los equipos de seguridad responder a las amenazas de manera coordinada y eficaz. • **Gestión en una sola consola:** La solución integrada debe proporcionar una única consola de gestión para EDR y ATP, permitiendo a los equipos de seguridad monitorizar, analizar y responder a amenazas desde una única interfaz.
43	Arquitectura e Integración del Componente EDR	La solución propuesta de Detección y Respuesta de Endpoint (EDR) debe utilizar un único agente unificado que se integre con la aplicación de Protección de Endpoints, proporcionando una postura de seguridad convergente para los dispositivos endpoint. El agente único debe proporcionar las siguientes capacidades: • Detección y prevención de amenazas en tiempo real. • Protección de endpoints (por ejemplo, antivirus, cortafuegos, etc.). • Capacidades EDR (por ejemplo, análisis conductual, detección de anomalías, etc.). • Integración fluida con la solución ATP.
44	Arquitectura e Integración del Componente EDR	El agente EDR deberá soportar operación lado a lado con múltiples plataformas de protección de endpoints (EPP) ampliamente utilizadas en el mercado, incluyendo soluciones de fabricantes reconocidos, sin generar conflictos operativos.

Ítem	Característica técnica	Descripción
45	Arquitectura e Integración del Componente EDR	La solución debe proporcionar una API al menos para las siguientes propuestas: • API para ejecutar acciones de remediación/respuesta en endpoints. • API para la recuperación de telemetría de endpoints etiquetados por sistemas de terceros. • API para la recuperación de información de alertas de aplicaciones por parte de sistemas de terceros.
46	Arquitectura e Integración del Componente EDR	La solución debe proporcionar la capacidad de almacenar todos los datos de telemetría de los endpoints localmente durante un mínimo de 15 días, con la opción de ampliar el periodo de almacenamiento según sea necesario.
47	Arquitectura e Integración del Componente EDR	La solución debe permitir la creación e importación de reglas de detección mediante formatos estructurados y estandarizados de uso común en la industria, facilitando la interoperabilidad y reutilización de reglas existentes.
48	Arquitectura e Integración del Componente EDR	La solución debe permitir el envío de archivos para escanear en un entorno Sandbox desde hosts protegidos que ejecuten sistemas operativos Windows y Linux. Esta función debe permitir: • Integración fluida con hosts protegidos para recopilar y enviar archivos para escanear. • Soporte para sistemas operativos Windows y Linux. • Envío automatizado de archivos al entorno Sandbox para su análisis. • Esta capacidad debería permitir a la solución detectar y analizar amenazas potenciales en hosts protegidos y proporcionar una capa adicional de seguridad y detección de amenazas.
49	Capacidades ANTI-APT (APT / SANDBOX)	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.
50	Capacidades ANTI-APT (APT / SANDBOX)	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.
51	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe soportar el análisis comprimido de objetos de múltiples niveles.
52	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware de la solución propuesta debe utilizar un entorno sandboxing multi-OS, que soporte múltiples sistemas operativos virtuales cliente tanto de arquitecturas x64 como x86.
53	Capacidades ANTI-APT (APT / SANDBOX)	El entorno Sandbox deberá soportar múltiples sistemas operativos ampliamente utilizados en entornos corporativos, incluyendo sistemas Windows y Linux en arquitecturas x86 y x64, permitiendo su actualización conforme evolucionen las versiones soportadas por el fabricante.
54	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de crear y gestionar dinámicamente máquinas virtuales (VMs) para cada sistema operativo compatible, permitiendo el análisis automatizado de muestras de malware en un entorno controlado y aislado.
55	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware también debe ser capaz de:

Ítem	Característica técnica	Descripción
		• Seleccionar automáticamente el sistema operativo más adecuado para el análisis en función de las características de la muestra de malware. • Permitir personalizar la configuración de las máquinas virtuales para imitar entornos reales y evadir técnicas de evasión de malware.
56	Capacidades ANTI-APT (APT / SANDBOX)	Recopila y analiza datos de telemetría de las máquinas virtuales para proporcionar información detallada sobre el comportamiento y las características del malware.
57	Capacidades ANTI-APT (APT / SANDBOX)	La solución deberá proporcionar integración con agentes de endpoint para facilitar la funcionalidad de Análisis Sandbox enviando archivos a un entorno sandbox para su análisis dinámico, permitiendo la detección de actividades maliciosas y comportamientos característicos de ataques dirigidos a la infraestructura informática de la organización.
58	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware debe proporcionar un motor de reglas de escaneo personalizable, que permita la definición condicional de qué objetos escanear en cada tipo de VM analizadora. El motor debe soportar lógica condicional, filtrado de objetos y actualizaciones dinámicas de reglas. El subsistema de Análisis Automatizado de Malware debe proporcionar la capacidad de definir reglas de escaneo condicionalmente qué objetos escanear o no escanear en una VM analizadora concreta.
59	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware debe proporcionar a los analistas resultados detallados, incluyendo: • Una representación gráfica del árbol de procesos, que muestra las relaciones entre procesos. • Datos sobre el tráfico web, incluyendo solicitudes y respuestas HTTP. • Datos sobre la comunicación DNS, incluyendo consultas y respuestas. • Este resultado debe presentarse de forma clara y accionable, permitiendo a los analistas comprender rápidamente el comportamiento y las características del malware.
60	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware de la solución debe poder funcionar con varios Centros de Análisis simultáneamente.
61	Capacidades ANTI-APT (APT / SANDBOX)	La solución Análisis Automatizado de Malware debe tener la opción de usar una conexión dedicada a Internet para permitir el análisis de comunicaciones salientes y módulos adicionales descargados.
62	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware debe ser capaz de simular las acciones del usuario final para forzar la ejecución de malware que dependan de disparadores del usuario final, como un clic de ratón, y permitir la comunicación por Internet para un mejor análisis de los objetos malware.
63	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de procesar y analizar archivos adjuntos en mensajes de correo, incluidos archivos protegidos por contraseña y documentos de oficina.
64	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe contar con una lista personalizable de contraseñas para desempaquetar archivos y documentos de oficina protegidos por contraseña.
65	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de obtener contraseñas para desempaquetar archivos protegidos por contraseña y documentos de oficina del cuerpo del mensaje de correo.
66	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware de la solución debe ser capaz de ocultarse frente al malware que evade el sandbox durante el análisis de objetos.
67	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware de la solución debe ser capaz de procesar manualmente los objetos enviados a través de la interfaz de gestión de soluciones.

Ítem	Característica técnica	Descripción
68	Capacidades ANTI-APT (APT / SANDBOX)	La solución deberá proporcionar orientación práctica o recomendaciones de respuesta ante alertas de seguridad generadas por la plataforma, con el fin de apoyar a los administradores en la investigación y remediación de incidentes.
69	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de recibir entradas para indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA) para clasificar y analizar eventos.
70	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe detectar tráfico de red potencialmente malicioso, como consultas DNS a Botnet C2 y otras comunicaciones.
71	Capacidades ANTI-APT (APT / SANDBOX)	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.
72	Capacidades ANTI-APT (APT / SANDBOX)	Los administradores de soluciones deben tener la opción de poner en lista blanca las reglas de detección de red si es necesario.
73	Capacidades ANTI-APT (APT / SANDBOX)	La solución deberá permitir la exportación en formato PCAP del tráfico de red asociado a eventos detectados, con fines de análisis forense.
74	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de soportar integración en modo de monitorización SPAN.
75	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe poder funcionar en modo de monitorización (fuera de banda), sin interferir con la comunicación entrante/saliente ni interrumpir los procesos empresariales.
76	Capacidades ANTI-APT (APT / SANDBOX)	El subsistema de Análisis Automatizado de Malware debe tener la capacidad de proporcionar la siguiente información al analista: • Informe completo de modificación de host disponible tras la ejecución en VM. • Copia del(los) binario(s) malware. • Metadatos de red que identifican las ubicaciones a las que el malware intenta comunicarse. • Información importante. • Capturas de pantalla de la actividad del escritorio.
77	Capacidades ANTI-APT (APT / SANDBOX)	La solución análisis automatizado de Malware debe ser capaz de examinar objetos utilizando múltiples instancias de servidor de subsistema para mejorar el tiempo de análisis.
78	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de reexaminar de forma inteligente eventos y objetos pasados utilizando la inteligencia más reciente para descubrir posibles amenazas previas.
79	Capacidades ANTI-APT (APT / SANDBOX)	Los veredictos obtenidos mediante el subsistema de análisis automatizado de Malware deben enriquecer la base de datos de reputación local utilizada por aplicaciones de soluciones EDR, soluciones ATP y Protección de Endpoints.
80	Capacidades ANTI-APT (APT / SANDBOX)	Los objetos detectados por el subsistema de Análisis de Malware deben ser bloqueados automáticamente para que no se ejecuten en endpoints protegidos si es necesario.
81	Capacidades ANTI-APT (APT / SANDBOX)	Las acciones sospechosas detectadas por el subsistema de análisis automatizado de Malware deben relacionarse con fases de ataque, técnicas de hackers y métodos de la matriz MITRE ATT&CK.
82	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe tener la capacidad de importar reglas YARA para su uso en el escaneo de objetos del tráfico de red, archivos enviados manualmente y escaneos en los endpoints.

Ítem	Característica técnica	Descripción
83	Capacidades ANTI-APT (APT / SANDBOX)	La solución ATP debe ser capaz de identificar infraestructuras C2 conocidas utilizando servicios de URL y reputación de dominio.
84	Capacidades ANTI-APT (APT / SANDBOX)	La solución ATP debe ser capaz de identificar infraestructuras de C2 previamente desconocidas utilizando el Sistema de Detección de Intrusiones. Las reglas de detección de comunicaciones maliciosas deben ser proporcionadas y actualizadas por el equipo experto del fabricante.
85	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe incluir el subsistema de Análisis Automatizado de Malware para detonar objetos sospechosos dentro de un entorno virtual controlado y así evaluar su nivel de amenaza.
86	Capacidades ANTI-APT (APT / SANDBOX)	La solución Análisis Automatizado de Malware debe proporcionar la capacidad de preparar y utilizar imágenes de VM personalizadas para el análisis dinámico de malware.
87	Capacidades ANTI-APT (APT / SANDBOX)	Múltiples Centros de Análisis deben poder conectarse a un único subsistema de Análisis Automatizado de Malware.
88	Capacidades EDR	Las funciones investigadoras deben incluir datos históricos de eventos del punto final principal (telemetría) para determinar los cambios ocurridos.
89	Capacidades EDR	El usuario de la solución (analista de seguridad) debe disponer de una herramienta automatizada para obtener una lista de archivos almacenados en una carpeta específica en un punto final, lista de procesos que se ejecutan en un punto final dado, volcado de memoria de procesos, volcado completo de memoria, imagen de disco, claves de registro, metaarchivos NTFS y lista de puntos automáticos.
90	Capacidades EDR	La solución debe proporcionar visibilidad sobre la posible propagación de amenazas dentro del conjunto de endpoints protegidos y su relación con eventos detectados en la red.
91	Capacidades EDR	Los detects de la solución de Protección de Endpoints deben proporcionar información adicional a la base de datos de telemetría para la solución EDR y estos datos deben ser buscables mediante la consola de analistes.
92	Capacidades EDR	El agente de la solución EDR debe tener protección contra manipulaciones.
93	Capacidades EDR	La solución debe tener la capacidad de ejecutar escaneos IOC dentro de una base de datos centralizada de telemetría recopilada en endpoints.
94	Capacidades EDR	La solución debe tener la capacidad de forzar la ejecución del escaneo IOC en todos los endpoints que cuenten con agente EDR instalado.
95	Capacidades EDR	La solución EDR debe proporcionar la capacidad de ejecutar escaneos YARA en los endpoints
96	Capacidades EDR	La solución EDR debe proporcionar una interfaz de búsqueda con funcionalidad avanzada para que los analistas puedan construir solicitudes de búsqueda sofisticadas contra bases de datos de telemetría.
97	Capacidades EDR	La solución EDR debe proporcionar medios para aislar la máquina del resto de la red en caso de emergencia, preservando la comunicación controlada con el servidor de administración y control de los agentes.
98	Capacidades EDR	La solución EDR debe proporcionar medios de remediación remota mediante agente (eliminación y cuarentena de archivos, eliminación de procesos, prevención de la ejecución o apertura de archivos concretos, etc.)
99	Capacidades EDR	La solución EDR debe ser capaz de detectar conexiones entrantes o salientes a infraestructura C&C desde los endpoints protegidos.
100	Capacidades EDR	Las alertas sobre detecciones deben enriquecerse automáticamente con datos contextuales relevantes como descripciones, clases de amenazas, prevalencia geográfica, etc.
101	Capacidades EDR	La solución deberá permitir etiquetar endpoints protegidos y activos críticos identificados para aplicar políticas diferenciadas.
102	Capacidades EDR	Las alertas y eventos generados por los endpoints protegidos deberán mapearse a técnicas de la matriz MITRE ATT&CK.

Ítem	Característica técnica	Descripción
103	Capacidades EDR	La solución deberá permitir la gestión e incorporación de indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA), aplicables a los endpoints protegidos y a los motores de análisis de red y sandbox según corresponda.
104	Capacidades NDR	La solución debe proporcionar una capacidad de análisis del tráfico de red, permitiendo a los usuarios: • Visualiza e inspecciona los eventos de tráfico de red en tiempo real • Analizar capturas de paquetes y flujos de red • Identificar posibles amenazas y anomalías de seguridad en el tráfico de red • Esta capacidad debería permitir a los equipos de seguridad obtener visión del tráfico de red, detectar amenazas potenciales y responder a incidentes de manera oportuna y eficaz.
105	Capacidades NDR	La solución proporcionará un inventario completo de dispositivos en la red local de la organización, incluyendo: • Información de la cuenta de usuario registrada en los sistemas operativos del dispositivo. • Historial de ejecución de archivos en dispositivos. • Espacios de direcciones de dispositivos (por ejemplo, direcciones IP, direcciones MAC).
106	Capacidades NDR	La solución permitirá mostrar los riesgos asociados a los dispositivos, facilitando la gestión proactiva de amenazas.
107	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 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.
108	Capacidades NDR	La solución debe proporcionar capacidades de respuesta de red, incluida la integración con dispositivos de comunicación de red, para permitir el aislamiento y contención sospechosos 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.
109	Capacidades NDR	La solución debe soportar direccionamiento IP dinámico de los dispositivos, asegurando un seguimiento y monitorización precisos.
110	Capacidades NDR	La solución proporcionará monitorización en tiempo real de la actividad de red de los dispositivos en un mapa de red, permitiendo la visualización del tráfico de red y posibles amenazas de seguridad.
111	Capacidades NDR	La solución permitirá un sondeo activo de dispositivos para enriquecer la información del dispositivo y construir un mapa topológico de red completo.
112	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.
113	Capacidades NDR	A efectos de la investigación y/o normativa de cumplimiento de incidentes cibernéticos, la solución debe proporcionar la capacidad de capturar y registrar el tráfico de red en bruto.
114	Capacidades NDR	El tráfico grabado puede capturarse en un formato que puede analizarse y reproducirse fácilmente, como PCAP (Captura de Paquetes).
115	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.

Ítem	Característica técnica	Descripción
116	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.
117	Capacidades NDR	La solución permitirá la búsqueda y recuperación de sesiones de red basándose en capturas de paquetes en el almacenamiento de tráfico.
118	Capacidades NDR	La solución permitirá exportar los paquetes individuales de red y los datos de sesión a un archivo para su análisis posterior.
119	Documentación	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.
120	Documentación	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 actualizaciones, parches y mejoras durante la vigencia del licenciamiento. Se debe presentar una certificación en donde se compruebe de lo solicitado.
121	Documentación	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.
122	Documentación	El proponente deberá presentar certificación vigente expedida por el fabricante que acredite su condición de 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.

Tabla 1. Especificaciones técnicas mínimas obligatorias

5. Requerimientos de desempeño:

La solución de detección, prevención y respuesta a nivel de red deberá garantizar condiciones mínimas de desempeño que permitan su adecuada operación dentro de la infraestructura tecnológica de la Universidad Distrital Francisco José de Caldas. La solución deberá cumplir como mínimo con las siguientes condiciones:

a. **Disponibilidad de la plataforma:** La solución deberá garantizar una disponibilidad mínima del 99,9 %, considerando los componentes de gestión, análisis y generación de alertas, salvo ventanas de mantenimiento previamente coordinadas con la supervisión del contrato.
b. **Tiempo de respuesta ante incidentes de soporte:** El servicio de soporte técnico deberá operar bajo un esquema 7x24, con tiempos de respuesta acordes a la criticidad del incidente reportado, garantizando atención oportuna a fallas que afecten la operación de la solución.
c. **Capacidad de procesamiento de tráfico:** La solución deberá contar con la capacidad necesaria para analizar el tráfico de red capturado desde los puntos estratégicos definidos (Core, DMZ y Data Center institucionales), permitiendo la detección de comportamientos anómalos y eventos de seguridad sin afectar la operación normal de la red institucional.

d. Escalabilidad: La solución deberá permitir el crecimiento de la capacidad de monitoreo o la incorporación de nuevos sensores o fuentes de tráfico, en caso de que la infraestructura institucional así lo requiera.

6. Proceso de implementación

La implementación de la solución deberá garantizar los siguientes aspectos:

a. Instalación y configuración: Verificación de la correcta instalación y configuración de todos los componentes de la solución sobre la infraestructura de servidores suministrada por la Universidad Distrital. El contratista deberá garantizar el correcto despliegue de la plataforma de gestión, sensores o colectores de tráfico y demás componentes necesarios para la operación de la solución.

b. 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.

c. 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.

d. 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.

e. 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.

f. Prueba de funcionamiento: 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. El licenciamiento deberá iniciar cuando esta prueba sea exitosa.

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

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

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:

a. 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.

b. 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, asegurando su corrección sin costo adicional para la entidad.

c. 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) 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) para la atención de incidentes o fallas relacionadas con la operación 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. **Actualizaciones de la solución**: 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.

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.

11. Anexos

Con el fin de garantizar la adecuada implementación, integración y desempeño de la solución, se informa a los oferentes que la Universidad Distrital Francisco José de Caldas adelantará un proceso de contratación estructurado en dos (2) componentes:

Componente 1: Licenciamiento de la solución de ciberseguridad (objeto del presente proceso).

Componente 2: Adquisición de servidores, requerido como infraestructura de soporte para la solución.

En este sentido, los oferentes deberán tener en cuenta que el componente de servidores se contratará mediante un proceso complementario. Por lo tanto, es obligatorio consultar las

especificaciones técnicas asociadas a dicho componente, las cuales se encuentran descritas en los anexos del estudio previo, con el fin de validar la compatibilidad, dimensionamiento e integración de la solución propuesta con la infraestructura tecnológica prevista.