ESPECIFICACIONES TÉCNICAS MINIMAS REQUERIDAS:

Con el fin de mejorar la red interna de comunicaciones y fortalecer la seguridad tecnológica. La Agencia distrital para la educación superior, la ciencia y la tecnología – Atenea, requiere:

1. RENOVACIÓN DEL SOPORTE Y LICENCIAMINETO DE LA PLATAFORMA FORTINET

GENERALIDADES

Actualmente la Entidad, cuenta con equipos de seguridad perimetral y herramienta de gestión de eventos, los cuales su licenciamiento y soporte están vigentes para el 2026, en tal sentido la "**ATENEA - Agencia Distrital Para la Educación Superior, la Ciencia y la Tecnología"**, requiere realizar la renovación y actualización del licenciamiento y soporte técnico de fábrica de los equipos relacionados a continuación, a partir de la fecha actual de renovación y hasta el 31 de octubre del 2027.

REFERENCIA	SERIAL	FECHA FIN SOPORTE ACTUAL
FortiGate-200F	FG200FT922924155	21/08/2026
FortiGate-200F	FG200FT922939483	17/07/2026
FortiAnalyzer-150G	FAZ15GT222000148	12/11/2026
FORTISWITCH 424E -CORE	S424ENTF23005376	6/11/2026
FORTISWITCH 424E - CORE	S424ENTF24000012	6/11/2026
FORTIAP-231G	FP231GTF23050504	6/11/2026
FORTIAP-431G	FP431GTY23012733	6/11/2026
FORTIAP-431G	FP431GTY23012736	6/11/2026
FORTIAP-431G	FP431GTY23012738	6/11/2026
FORTIAP-431G	FP431GTY23012755	6/11/2026
FORTIAP-431G	FP431GTY23012756	6/11/2026
FORTIAP-431G	FP431GTY23012758	6/11/2026
FORTIAP-431G	FP431GTY23012779	6/11/2026
FORTIAP-431G	FP431GTY23012784	6/11/2026
FORTIAP-431G	FP431GTY23012786	6/11/2026
FORTIAP-431G	FP431GTY23020356	27/12/2026
FORTIAP-431G	FP431GTY23020382	27/12/2026
FORTIAP-431G	FP431GTY23033155	27/12/2026

1. RENOVACIÓN DEL SOPORTE Y LICENCIAMINETO DE LA PLATAFORMA FORTINET

FORTISWITCH FS-124F-FPOE	S124FFTF24010775	27/12/2026
FORTISWITCH FS-148F-FPOE	S148FFTF21017599	6/11/2026
FORTISWITCH FS-148F-FPOE	S148FFTF21019563	6/11/2026
FORTISWITCH FS-148F-FPOE	S148FFTF23077625	6/11/2026
FORTISWITCH FS-148F-FPOE	S148FFTF23077635	6/11/2026
FORTISWITCH FS-148F-FPOE	S148FFTF24002864	27/12/2026
FORTISWITCH FS-148F-FPOE	S148FFTF24003132	27/12/2026

- Para las plataformas de seguridad Next Generation Firewall (NGFW) se requiere que la renovación sea para el licenciamiento **"UTP"**

- Para la plataforma de gestión de logs y eventos centralizados FortiAnalyzer 150G se requiere que la renovación sea para el siguiente licenciamiento:
  - **Enterprise + Forticare Premium, licenciamiento actual**

- Incluir FortiAnalyzer IA (Servicio de seguridad impulsado por IA generativa que utiliza modelos de lenguaje grandes (LLM) para brindar asistencia en tiempo real).

- Pqra la soluciones de Networking y seguridad LAN FortiSwitch y FortiAP se requiere que la renovación sea para el siguiente licenciamiento:
  - **Forticare Premium**

- El tiempo de renovación se debe contar a partir del siguiente día de la fecha fin del soporte actual

- El soporte se debe prestar en un esquema 7x24: Atención a incidentes operativos, los cuales se refieren a una interrupción no planificada de un servicio, o reducción en la calidad de un servicio prestado para la plataforma Fortinet hasta el 31 de octubre del 2027.

- Gestión de requerimientos 5x8: Atención a requerimiento de cambios de configuración solicitados por parte de la entidad, para la plataforma Fortinet hasta el 31 de octubre del 2027.

- El soporte debe contemplar remplazo de equipos por unos totalmente nuevos y mínimo de las mismas características y completa compatibilidad con la

1. RENOVACIÓN DEL SOPORTE Y LICENCIAMINETO DE LA PLATAFORMA FORTINET

infraestructura actual, en caso de que los equipos actuales presente algún tipo de daño físico.

AFINAMIENTO Y/O ACTUALIZACION DE LA PLATAFORMA FORTINET

El oferente debe realizar un afinamiento y actualización de software anual durante la vigencia del soporte del fabricante a la configuración de toda la plataforma FORTINET, incluye Firewall, Switch, Acces point y Fortianalyzer,

•Revisión de la configuración actual
•Recomendación de mejores prácticas para ajuste a la configuración
•Actualización de firmware (recomendada por el fabricante y estable
•Configuración de la recomendaciones realizadas y activación de nuevas funcionalidades (si aplica)

Esta actividad se realizará durante la vigencia del soporte del fabricante en coordinación con el supervisor y en horario no hábil para la entidad.

MODULOS TRANSCEIVERS SFP+

Se requiere la **actualización de los enlaces de fibra óptica actualmente operando a 1 Gbps**, los cuales interconectan los **switches de acceso con la capa de distribución**, con el fin de incrementar la capacidad de transmisión y soportar el crecimiento de la demanda de tráfico de red. Para tal efecto, se plantea la **migración de dichos enlaces a una velocidad de 10 Gbps**.

En consecuencia, se requiere el suministro de **doce (12) módulos transceiver SFP+ 10GE**, con las siguientes características técnicas mínimas:

- Tipo: **SFP+ 10 Gigabit Ethernet**
- Medio: **Fibra óptica multimodo (MMF)**
- Longitud de onda: **850 nm**
- Conector: **Dúplex LC**
- Alcance acorde con enlaces MMF en infraestructura interna

Los transceivers suministrados deberán ser **totalmente compatibles con la plataforma FORTINET instalada**, garantizando su correcto funcionamiento sin degradación del desempeño, asegurando la estabilidad de los enlaces, la continuidad del servicio y el

1. RENOVACIÓN DEL SOPORTE Y LICENCIAMINETO DE LA PLATAFORMA FORTINET
cumplimiento de las capacidades de conmutación y agregación definidas en la arquitectura de red institucional. **Instalación y puesta en operación de transceivers SFP+** Los **transceivers SFP+ suministrados deberán ser instalados en los equipos de red correspondientes**, reemplazando los módulos actualmente en operación. El proveedor deberá realizar **todas las configuraciones técnicas necesarias** en los dispositivos involucrados para garantizar la correcta negociación de velocidad, estabilidad del enlace y compatibilidad con la infraestructura existente. Una vez realizada la instalación y configuración, los enlaces deberán **quedar totalmente operativos**, funcionando a **10 Gbps**, sin degradación del servicio, asegurando la continuidad operativa de la red, la interoperabilidad con los equipos FORTINET de la entidad y el cumplimiento de los parámetros definidos en la arquitectura tecnológica institucional, el cableado estructurado y fibras requeridas serán provistas por la entidad. La actividad de instalación y puesta en operación se realizará en una ventana de mantenimiento coordinada con el supervisor y en horario no hábil para la entidad. La Entidad garantizara la disponibilidad de la infraestructura bajo su responsabilidad, incluyendo el cableado estructurado, fibra óptica y demás componentes que hacen parte de la infraestructura existente, cumpliendo con las especificaciones técnicas requeridas para operar *a* **10 Gbps**.

La entidad requiere renovar el servicio de detección de tráfico anómalo y en tiempo real en la red LAN con características de inteligencia artificial para la toma de decisiones a través del aprendizaje automático.

2. SERVICIOS DE SISTEMA DE DETECCION DE AMENAZAS CON INTELIGENCIA ARTIFICIAL	
SISTEMA DE DETECCIÓN DE AMENAZAS	El servicio debe estar compuesto por hardware, software, trasferencia de conocimiento y servicios especializados que permite la puesta en marcha de la solución que mitigue los riesgos informáticos de la Entidad.

2. SERVICIOS DE SISTEMA DE DETECCION DE AMENAZAS CON INTELIGENCIA ARTIFICIAL	
	Actualmente la Entidad cuenta con un centro de datos de nube de Oracle, donde se encuentras los servicios críticos de la Entidad y una oficina principal El proveedor deberá renovar el servicio con licenciamiento total de la solución para 500 dispositivos por **1 año**, contados a partir la fecha del acta de inicio del contrato. El servicio para renovar deberá estar basada en hardware appliance, es decir, hardware de propósito específico destinado a alojar el sistema de seguridad requerido con las condiciones de endurecimiento propias de un sistema de seguridad. El servicio debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice e identifique las amenazas o incidentes que están ocurriendo en la red. Después del período de aprendizaje inicial, la tecnología debe proporcionar automáticamente un seguimiento de auditoría completo de todos los dispositivos en el entorno, clasificando previamente al menos el tipo de dispositivo, el nombre de host, la dirección MAC, la primera y la última vez que se detectó el dispositivo en la red El servicio debe basarse en el análisis de comportamiento y correlación inteligente pudiendo detectar: ● Toda conectividad inusual en la red. ● Todas las actividades anómalas en la red. Ser capaz de hacer un seguimiento detallado del dispositivo, indicando incluso su historial de dirección IP, uso del protocolo DHCP, etc. Tener la capacidad de hacer un seguimiento detallado del usuario indicando incluso todos los nombres de host asociados a unas determinadas credenciales. Identificar un volumen de conexiones significativamente inusual.

2. SERVICIOS DE SISTEMA DE DETECCION DE AMENAZAS CON INTELIGENCIA ARTIFICIAL	
	Identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo. El servicio debe alertar automáticamente sobre todas las actividades inusuales y anómalas en la red La solución debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la línea de base normal de comportamiento, así: • La línea base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno • Debe funcionar completamente en función del comportamiento, donde no se permitan las tecnologías que hacen uso de reglas y / o firmas Se deberá poder integrar el proceso de Threat Hunting automatizado para que otros servicios vía API puedan solicitar informes de cacería de amenazas de manera automatizada. Se deben poder solicitar investigaciones autónomas y a demanda a la inteligencia artificial, donde el disparador pueda ser una anomalía ya detectada o una simple investigación a demanda. El proceso de Threat Hunting deberá proporcionar un informe base entregado por la inteligencia artificial y uno adicional con la información de contexto y otras investigaciones adicionales realizadas por los analistas humanos. El proceso deberá tener la capacidad de realizar investigaciones continuas 24/7 y en tiempo real de las anomalías detectadas por la inteligencia artificial Se deberán proponer los reportes estadísticos del servicio a nivel ejecutivo. Se deberán acordar los reportes de los Threat Hunting y su respectiva evidencia con al menos un reporte por cada investigación realizada.

2. SERVICIOS DE SISTEMA DE DETECCION DE AMENAZAS CON INTELIGENCIA ARTIFICIAL	
	Se deberán realizar procesos de Threat Hunting manuales basados en TTP's mitre de manera recurrente, identificando qué anomalías detectadas por la plataforma de Inteligencia Artificial hacen parte de las técinas buscadas para cada ejercicio de Treath Hunting propuesto. La solución debe permitir la personalización avanzada de la tecnología, permitiendo considerar múltiples parámetros de datos al verificar un determinado comportamiento, entre los parámetros debería ser posible tener las siguientes opciones: conexiones externas, conexiones internas, transferencia de datos, datos externos transferencia, conexiones SMB, conexiones de puerto cerrado, difusiones, dispositivos conectados, transferencia de datos (cliente), transferencia de datos (servidor), entre otras métricas relevantes. La solución debe utilizar varios algoritmos de inteligencia artificial, así como varias técnicas de Machine Learning como: Deep Learning, Machine Learning supervisado y Machine Learning no supervisado. La tecnología de identificación de amenazas de la solución no debe basarse en firmas, ni reglas, ni heurística, ni sandboxing. Debe estar puramente basada en algoritmos avanzados de Machine Learning e Inteligencia Artificial. La solución no depende de una conexión hacia Internet para realizar sus operaciones de inteligencia y análisis. Debe funcionar completamente en función del comportamiento, donde no se permitirán las tecnologías que hacen uso de reglas, firmas y/o Indicadores de Compromiso (IoC's) La solución debe tener la capacidad de modelar el comportamiento normal a nivel de usuario, dispositivos y red y a partir de estos identificar de forma autónoma las anomalías que corresponden a brechas de seguridad. La solución debe poder realizar un aprendizaje autónomo del comportamiento normal de la red sin requerir previo conocimiento del historial de comportamiento anómalo, con la posibilidad de identificar amenazas. La tecnología debe tener la capacidad de detectar amenazas internas y externas

2. SERVICIOS DE SISTEMA DE DETECCION DE AMENAZAS CON INTELIGENCIA ARTIFICIAL	
	La tecnología debe ser auto-configurable, es decir, debe tener capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real. La solución debe tener capacidad de detectar como mínimo los siguientes tipos de brechas de seguridad: ● Ataques de tipo botnet ● Propagación de gusanos ● Ataques de ransomware ● Infiltración y exfiltración de datos Troyanos bancarios ● Credenciales comprometidas ● Minería de bitcoins ● Malware ● Ataques de DDoS a través de dispositivos IoT ● Amenazas avanzadas persistentes (APT) La herramienta debe ser on premise, no se aceptan soluciones que necesiten de la nube para hacer los análisis de la información, cualquier configuración remota debe ser consultada y autorizada con la entidad. La solución contra amenazas deberá funcionar sin necesidad de tener conexión a una nube de inteligencia de amenazas, sandbox o cualquier consola en general que se encuentre en la nube o deba recolectar información desde la nube pública. La herramienta debe ser tipo appliance no se aceptarán equipos que involucren la instalación de agentes en los dispositivos a monitorear (agent-less). La solución debe poder reconocer nuevas amenazas que no hayan sido advertidas previamente (Zero Day).
VISUALIZACIÓN DE RED	● La solución debe poseer una interfaz de visualización amigable, que debe ser accesible vía web. ● La interfaz de visualización debe permitir tener visibilidad gráfica de cualquier elemento de la red con gran profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real. No deberá necesitar compartir datos con una

2. SERVICIOS DE SISTEMA DE DETECCION DE AMENAZAS CON INTELIGENCIA ARTIFICIAL	
	nube de seguridad global para obtener su inteligencia de seguridad. ● La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso. ● La solución debe ser capaz de agrupar automáticamente los dispositivos en grupos y/o grupos por su similitud de comportamiento ● La solución debe tener una barra de búsqueda que permita buscar inmediatamente un dispositivo, IP, subred o host de red La solución debe tener una interfaz de usuario donde se pueda consultar el estado completo del sistema, incluyendo: a. La versión del software, el espacio en disco utilizado, el consumo de CPU y el consumo de memoria. b. El detalle de todas las interfaces activas y el tráfico respectivo recibido a través de cada una de ellas c. El ancho de banda total procesado, el ancho de banda promedio procesado hasta la fecha, el ancho de banda registrado en los últimos periodos de tiempo. d. Un análisis detallado de todo el tráfico recibido en el dispositivo y la última vez que se identificaron los protocolos principales, entre ellos HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, etc. La solución debe tener visibilidad en tiempo real de los siguientes datos correspondientes a la red: ● Cantidad de servidores o Cantidad de estaciones cliente ● Cantidad de credenciales de usuario o Tráfico de red ● La interfaz de visualización debe poseer una barra de búsqueda que permita identificar de manera rápida cualquier elemento de la red bajo los siguientes criterios: ● Dirección IP o Tipo de dispositivo o Función o protocolo conocido. ● Tipo de dispositivo o Nombre del dispositivo ● Cuando se hace búsqueda de un dispositivo, la interfaz debe poder mostrar la información de éste en detalle incluyendo: Dirección IP, dirección MAC, sistema operativo, logs de eventos, logs de brechas de seguridad identificadas, historial de conexiones, lista de dispositivos similares.

2. SERVICIOS DE SISTEMA DE DETECCION DE AMENAZAS CON INTELIGENCIA ARTIFICIAL	
	• La interfaz debe permitir la visualización de todas las subredes, así como todos los dispositivos que las conforman. Debe permitir la visualización de la subred de manera gráfica en tiempo real, mostrando el esquema de conexiones entre los dispositivos. Las subredes deben poder visualizarse en un mapa global que permita conocer la ubicación real de cada una.
VISIBILIDAD DE AMENAZAS	• La interfaz debe mostrar las amenazas que se van identificando en la red en tiempo real, con el detalle de eventos de cada amenaza generados por la herramienta, así como vistas gráficas que permitan ver el comportamiento de la amenaza en el tiempo. • La solución debe proporcionar filtros simples y rápidos para permitir el análisis de eventos informáticos por parte de Usuarios, Dispositivos y tipo de evento. • La interfaz debe poder mostrar la amenaza de manera gráfica y en tiempo real. • Las amenazas identificadas deben tener un nivel de clasificación según su criticidad y debe contar con un código de colores asociado a cada nivel. • La interfaz debe brindar la posibilidad de investigación de alertas en profundidad en tiempo real, de manera gráfica y mediante eventos. • La solución debe tener una función que permita el análisis retrospectivo de los registros del incidente, devolviendo la conexión en segundos, minutos, horas o días antes de que se haya identificado una anomalía • La interfaz debe poseer herramientas o funcionalidades que permitan la investigación forense al mayor nivel de detalle de cualquier amenaza identificada, sin necesidad de uso de herramientas externas. • La solución debe ser capaz de agrupar las anomalías de manera inteligente y por nivel de criticidad. • La solución debe contar dentro la su propia interface con herramientas tipo Punycode Convertor, RegEx Tester, Base64 Convertor, JS Beautifie ,Epoch Converter , Facilitando el análisis de los incidentes. • La interfaz de visualización debe permitir tener visibilidad gráfica en 3D de cualquier elemento de la red con gran

	profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real. La visualización de cualquier elemento en la red debe ser en tiempo real y también debe existir la posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud preciso.
ARQUITECTURA DE LA SOLUCIÓN	La renovación debe contemplar el hardware y software de la solución debe ser centralizada, es decir, debe contar con una única interfaz de administración y visualización, desde la cual se pueda gobernar toda la solución y monitorear todo el entorno. ● La solución debe ser centralizada, es decir, debe contar con una única interfaz de administración y visualización, desde la cual se pueda gobernar toda la solución y monitorear todo el entorno. ● El análisis del tráfico mediante los algoritmos de Machine Learning e Inteligencia Artificial debe realizarse de manera centralizada y a la totalidad del tráfico proveniente del datacenter Principal ● El equipo que conforma el servicio debe poder estar fuera de línea, es decir, la recepción del tráfico de red debe hacerse a través de puertos pasivos (spam port), de tal manera de no cause retardos en el desempeño de la red. ● La solución debe realizar un análisis completo del tráfico. ● Se debe considerar los siguientes datos para el dimensionamiento del servicio a renovar (appliance especifico propio del fabricante): ● Cantidad de appliance como servicio: máximo dos (2) ● Conexiones por minuto 30.000 ● Troughput: 500 Mbps ● Cantidad de dispositivos a analizar: 500 ● Unidades de Rack por equipo: 1U ● La herramienta debe soportar los siguientes modos de implementación: Port mirror (SPAN PORT)
NOTIFICACIONES	● La solución debe contar con la capacidad de poder notificar las amenazas a través de correos electrónicos. ● La herramienta debe contar con una interfaz móvil disponible para Android y iOS, activa 7x24 que acelere las tareas de mitigación de riesgos mediante el envío de notificaciones push

	para dar aviso de amenazas en proceso y la posibilidad de confirmar acciones de respuesta autónoma.
ADMINISTRACIÓN	• La herramienta debe ser capaz de realizar backup y restore de la configuración, permitiendo al administrador programar la realización de los backups en el momento deseado. • Los backups deben poder ser transferidos a un repositorio vía SFTP o alguna tecnología de transferencia equivalente, es decir, que considere las medidas de seguridad bajo protocolos aceptados por la industria

CONTENCIÓN	• Para la contención y bloqueos de ataques, se debe utilizar el mismo equipo renovado en la solución de detección de amenazas, no se permite equipos (físicos o virtualizados) adicionales.
	• La solución debe estar en la capacidad de responder frente a incidentes de forma autónoma, esto es a partir del aprendizaje obtenido la inteligencia artificial debe decidir qué debe bloquear y como debe hacerlo, no debe utilizar configuraciones ni políticas predefinidas para realizar el bloqueo y debe bloquear únicamente el tráfico asociado a la amenaza mientras permite que el tráfico restante (no anómalo) siga fluyendo.
	  • La solución debe permitir integrarse con la infraestructura de seguridad existente, permitiendo optimizar la detección de amenazas y automatizando la mitigación de estas.
	  • Las acciones de bloqueo deben ser generadas con la precisión necesaria para interrumpir exclusivamente el tráfico que corresponde a las acciones maliciosas detectadas, de manera que no se afecte al tráfico de las actividades normales de los dispositivos involucrados.
	  • La solución debe tener capacidad para bloquear tráfico Norte-Sur y Este-Oeste de forma automática sin la instalación de dispositivos de control adicionales.
	  • La solución debe tener capacidad de determinar automáticamente como bloquear el tráfico sin causar mayor impacto a la organización utilizando inteligencia artificial, bloqueando conexiones específicas a través del envío de TCP-RST sin necesidad de integraciones con la infraestructura de la entidad.
	  • El bloqueo de conexiones a través de TCP-RST no debe necesitar más appliance físicos para su ejecución, se debe usar el mismo appliance de detección.
	  • La solución con la que se prestará el servicio debe poder ser configurada en modo pasivo-monitoreo o modo

	activobloqueo según la configuración predeterminada definida en conjunto con el personal de la entidad ● Deberá ser gestionable desde la misma interfaz gráfica (GUI) de detección de la solución.
PERIODO DE VIGENCIA	La solución deberá ser renovada por un periodo de **1 año**, contados a partir de la fecha del acta de inicio del contrato.
CAPACITACIÓN	● El fabricante debe tener un portal de capacitaciones sin costo adicional, donde encuentre capacitaciones técnicas sobre la solución ofertada, estás capacitaciones deben ser en español, las personas de la entidad deben poder inscribirse a estos cursos y tomarlos en vivo y en directo con un capacitador del fabricante, el fabricante debe tener disponibilidad de estos cursos al menos 2 veces al mes dentro del portal de capacitaciones.

BALLESTEROS CASTAÑEDA CARLOS ANDRES

Firmado digitalmente por BALLESTEROS CASTAÑEDA CARLOS ANDRES

CARLOS ANDRÉS BALLESTEROS CASTAÑEDA
Subgerente - Subgerencia de Tecnologías de la Información y las Comunicaciones

Elaboró: Juan Carlos Moreno. - Contratista Subgerencia de Tecnologías de la información y las comunicaciones.