ANEXO 1. FICHA TÉCNICA.
SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO
DIRECCIÓN DE GESTIÓN CORPORATIVA - SUBDIRECCIÓN DE INFORMÁTICA Y SISTEMAS

Objeto: Renovar licenciamiento, soporte y garantia de la solución de ciberseguridad instalada en la red de la SDDE.

CARACTERÍSTICAS GENERALES	
Denominación técnica del bien	Renovar licenciamiento, soporte y garantia de la solución de ciberseguridad.
Unidad de medida	Unidad
Descripción General	La Entidad está interesada en renovar licenciamiento, soporte y garantia de la solución de ciberseguridad.
Cantidad	1.000 licencias para soportar y monitorear los dispositivos de la red LAN e Inalámbrica.
CÓDIGOS UNSPSC	43233203, 43222503, 81111812
SISTEMA DE DETECCIÓN DE AMENAZAS	
1	La licencia del **FortiNDR-1000F appliance** debe ser capaz de identificar cualquier amenaza anómala en la red en tiempo real a través del aprendizaje automático e inteligencia artificial.
2	Contar con autorización del fabricante o su representante, para comercializar la marca y brindar las soluciones requeridas. El proponente deberá aportar una certificación dirigida a la entidad, donde se evidencie que es un canal autorizado por el fabricante de la solución
3	La solución 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.
4	La solución 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. * Identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo.
5	La solución debe alertar automáticamente sobre todas las actividades inusuales y anómalas en la red.
6	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.
7	La herramienta debe utilizar mecanismos adecuados con el fin de validar los comportamientos anómalos en la red. La solución debe proporcionar visibilidad completa de la red, incluidas las tecnologías tradicionales y no tradicionales.
8	La solución debe poder identificar cualquier comportamiento anómalo en el entorno y alertar sobre estos comportamientos en tiempo real
9	La solución debe ser capaz de identificar cualquier dispositivo nuevo en la red
10	Capacidad de realizar consultas a los datos capturados y almacenados en el hardware de uso específico (appliance).
11	Debe basarse en mecanismos adecuados analizando y correlacionando múltiples dimensiones distintas dentro del paquete.
12	La solución debe poder realizar una captura de paquetes en tiempo real que permita un análisis exhaustivo del incidente en el momento de su ocurrencia, así como ofrecer la opción de analizar el paquete tanto en Wireshark como dentro de su propia interfaz de usuario.
13	La solución debe permitir la personalización y adaptación del aprendizaje automático a condiciones y características específicas de la red.
14	Ser completamente automatizada, no debe requerirse de reglas o intervención humana para instruir a la solución sobre cómo utilizar los logs y flows recolectados para correlacionar y determinar ataques en tiempo real.
15	Debe realizar un análisis completo del tráfico (No análisis parciales de los paquetes p.e: sflow, jflow, netflow, Syslog)

16	La solución debe permitir la integración con LDAP o Directorio Activo
17	La solución debe permitir exponer la información recolectada a través de una interfaz web o via REST API, para que admita integraciones con otros elementos de seguridad.
18	La tecnología deberá proporcionar la capacidad de realizar procedimientos automatizados por parte del proveedor de la solución para la cacería de amenazas basados en inteligencia artificial con al menos las siguientes capacidades: * Procesos de Threat Hunting basados en anomalías de comportamiento detectadas por la inteligencia artificial. * Los procesos de Threat Hunting deberán indicar las fases del ciberataque en lo que se hayan visto la/las anomalías detectadas en el comportamiento. * El proceso de Threat Hunting deberá poder correlacionar anomalías detectadas dentro de la misma plataforma de IA e identificar si pertenecen o no a un ataque más complejo. Se deben validar con otras fuentes de información que llegan al correlacionador para dar mayor contexto a los hallazgos identificados por la inteligencia Artificial. * 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 dLa solución a nivel ejecutivo. * Se deberán acordar los reportes de los Threat Hunting y sus respectivas evidencias con al menos un reporte por cada investigación realizada. * 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
19	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, 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.
20	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.
21	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.
22	La solución no debe depender de una conexión hacia Internet para realizar sus operaciones de inteligencia y análisis.
23	Debe funcionar completamente en función del comportamiento.
24	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.
25	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 desde el primer día de instalación.
26	La solución nunca debe dejar de aprender autónomamente del comportamiento de red de la entidad, no se permiten soluciones con aprendizaje estático que sea configurado por la entidad.
27	La tecnología debe tener la capacidad de detectar amenazas internas y externas.
28	La tecnología debe ser auto-configurable, es decir, debe tener capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real.

<table>
<tr><td>29</td><td>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
*Credenciales comprometidas
*Botnets
*Malware
*Ataques de DDoS a través de dispositivos IoT
*Amenazas avanzadas persistentes (APT)</td></tr>
<tr><td>30</td><td>La solución contra amenazas deberá funcionar sin depender 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.</td></tr>
<tr><td>31</td><td>Deberá coenctarse a fuentes externas de Inteligencia de Amenazas para mejorar su inteligencia de seguridad.</td></tr>
<tr><td>32</td><td>La herramienta debe ser tipo appliance no se aceptarán equipos que involucren la instalación de agentes en los dispositivos a monitorear (agent-less).</td></tr>
<tr><td>33</td><td>La solución debe poder reconocer nuevas amenazas que no hayan sido advertidas previamente (Zero Day).</td></tr>
<tr><td colspan="2">PRODUCTOS SOLICITADOS</td></tr>
<tr><td>34</td><td><table><tr><th>Ítem</th><th>Cantidad</th><th>Descripción</th></tr><tr><td>a)</td><td>1 (software)</td><td>Licencias para soportar y monitorear hasta 1000 dispositivos de la red LAN e Inalámbrica.</td></tr><tr><td>b)</td><td>1 (por 12 meses)</td><td>Soporte y garantía para el equipo de la SDDE</td></tr></table></td></tr>
<tr><td></td><td>Debe incluir:
FortiCare Support
Firmware & General Updates
NDR Service</td></tr>
<tr><td colspan="2">VISUALIZACIÓN DE RED</td></tr>
<tr><td>35</td><td>La solución debe poseer una interfaz de visualización amigable, que debe ser accesible vía web.</td></tr>
<tr><td>36</td><td>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.</td></tr>
<tr><td>37</td><td>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.</td></tr>
<tr><td>38</td><td>La solución debe ser capaz de agrupar automáticamente los dispositivos en grupos y/o grupos por su similitud de comportamiento.</td></tr>
<tr><td>39</td><td>La solución debe tener una barra de búsqueda que permita buscar inmediatamente un dispositivo, IP, subred o host de red.</td></tr>
<tr><td>40</td><td>La solución debe tener una interfaz de usuario donde se pueda consultar el estado completo del sistema, incluyendo:
*La versión del software, el espacio en disco utilizado, el consumo de CPU y el consumo de memoria.
*El detalle de todas las interfaces activas y el tráfico respectivo recibido a través de cada una de ellas
*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.
*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.</td></tr>
<tr><td>41</td><td>La solución debe tener visibilidad en tiempo real de los siguientes datos correspondientes a la red:
* Cantidad de servidores
* Cantidad de estaciones cliente
* Tráfico de red</td></tr>
</table>

42	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 * Tipo de dispositivo * Función o protocolo conocido. * Tipo de dispositivo * Nombre del dispositivo
43	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.
44	La interfaz debe permitir la visualización de todos los componentes de la red en tiempo real, así como todos los dispositivos que las conforman.
VISIBILIDAD DE AMENAZAS	
45	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.
46	La solución debe proporcionar filtros simples y rápidos para permitir el análisis de eventos informáticos por parte de usuarios, dispositivos y tipo de evento.
47	La interfaz debe poder mostrar la amenaza de manera gráfica y en tiempo real.
48	Las amenazas identificadas deben tener un nivel de clasificación según su criticidad y debe contar con un código de colores asociado a cada nivel.
49	La interfaz debe brindar la posibilidad de investigación de alertas en profundidad en tiempo real, de manera gráfica y mediante eventos.
50	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
51	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.
52	La solución debe ser capaz de agrupar las anomalías de manera inteligente y por nivel de criticidad.
53	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	
54	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.
55	La solución debe realizar un análisis completo del tráfico.
56	La solución deberá cumplir como algunos de los siguientes estándares de seguridad: * UL 60950-CSA 60950, EN 60950, IEC 60950 CB Certicate & Report, IEC 60950 ó * FCC Part 15 Class A, RCM, VCCI, UL/cUL, CB
57	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.
58	Permitir integrarse con la infraestructura de seguridad existente (UTM9 sophos) e integrar con los demás componentes de la red de la entidad vía API, permitiendo optimizar la detección de amenazas y automatizando la mitigación de las mismas
59	Soportar de forma directa o con integraciones que las acciones de mitigación sean 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.
60	Capacidad para detectar el tráfico Norte-Sur y Este-Oeste de forma automática, mitigando de forma directa o a través la integración con las herramientas de la entidad
61	Capacidad de determinar automáticamente y tomar acciones de mitigación sin causar mayor impacto a la organización, utilizando inteligencia artificial, permitiendo el bloqueo de conexiones específicas a través del envío de TCP-RST o con integraciones con la infraestructura de la entidad.
62	Deberá ser gestionable desde la misma interfaz gráfica (GUI) de detección de la solución.
NOTIFICACIONES	
63	La solución debe contar con la capacidad de poder notificar las amenazas a través de correos electrónicos.
ADMINISTRACIÓN	
64	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.
65	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.

PERIODO DE VIGENCIA	
66	El licenciamiento, soportes y garantia por un periodo de doce (12) meses
SOPORTE DEL FABRICANTE Y DEL CANAL	
67	El fabricantedeberá brindar las actualizaciones de software sin costo adicional durante el periodo de vigencia del contrato.
68	El fabricante, a través de su soporte oficial, deberá brindar el acompañamiento técnico requerido para el apoyo y mitigación de incidentes de seguridad durante la vigencia del contrato de soporte
69	En caso de falla del equipo, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o en su defecto un equipo de reemplazo sin costo adicional, de acuerdo con las condiciones del contrato de soporte (RMA) vigente; el canal podrá apoyar en la gestión del caso ante el fabricante
70	El fabricante, a través de su soporte, brindará asistencia técnica para la resolución de incidentes y consultas de configuración dentro del marco del soporte estándar
71	Se debe entregar junto a la oferta, un certificado del fabricante dirigido a la entidad, indicando que es un socio o partner autorizado para brindar las soluciones de este fabricante.

ADRIANA MONTOYA RIOS
Subdirectora de Informática y Sistemas