1. OBJETO

DTC5 CONTRATAR LA RENOVACIÓN DEL LICENCIAMIENTO, GARANTÍA Y SOPORTE PARA LAS SOLUCIONES DE SEGURIDAD INFORMÁTICA Y/O MONITOREO Y/O ANALÍTICA DE FORTINET Y CACERÍA DE AMENAZAS POR MEDIO DE SEÑUELOS O DECOYS TIPO DECEPTOR PARA LA PROTECCIÓN PROACTIVA DE LA INFRAESTRUCTURA TECNOLÓGICA DE TRANSMILENIO S.A., SOPORTADA EN ARQUITECTURA FORTINET.

1.1. Alcance del Objeto

TRANSMILENIO S.A con el fin de mantener su infraestructura tecnológica actualizada, como apoyo básico para la operación de los procesos y procedimientos que ejecuta la Entidad en cumplimiento de sus funciones misionales, estratégicas y de apoyo, además de propender por el mantenimiento y correcta aplicación de controles que soportan la seguridad de los sistemas de información y la continuidad de los servicios con los que cuenta actualmente el ente gestor, requiere renovar el esquema licenciamiento y el soporte de la solución de monitoreo y analítica de disponibilidad y ciberseguridad de la Entidad, en la cual se encuentran equipos tecnológicos de logs, reportes y monitoreo de la experiencia digital fortinet, ubicados en nube y en el data center administrativo de TRANSMILENIO S.A.

El objeto del contrato implica los siguientes compromisos a cargo del CONTRATISTA:

- Renovar el licenciamiento específico de las soluciones Fortimonitor y Fortianalyzer de acuerdo con las siguientes especificaciones:

EQUIPO	CANTIDAD	FUNCIONALIDADES.
Monitoreo de la Experiencia Digital FortiMonitor	1	• FortiMonitor for 225 instances, including FortiCare Premium • Digital Experience Monitoring (DEM) for 125 Instances. • Devices/Servers for 100 Instances. • Total: 225 Instances.
Consola de Reportes y Logs FortiAnalizer	1	• FortiAnalyzer Attack Surface Security, para el monitoreo de la postura de seguridad desde la misma herramienta.
Solución tipo Deceptor VM	1	• • Suscripción tipo deceptor VM por 10 Meses incluyendo: license for Deception Decoys, Deception Lures plus Services Subscriptions (ARAE, AV, IPS, and Web Filtering). 12 network VLAN. Serial Number: FDCVMSTM24000091 • • Windows License Expands: Licensed Windows VM capacity Total 4. (2) Win7 and (2) Win10 license added.

- Las renovaciones son requeridas por un periodo de diez (10) meses en un esquema 7 x 24 ante fabricante y con las funcionalidades solicitadas de las plataformas para los equipos mencionados, garantizando las suscripciones de seguridad de los equipos durante el tiempo contratado e incluyendo acceso a soporte técnico de fábrica en esquema 7x24 y reemplazo de hardware (RMA) en caso de falla de este, para los elementos que aplique. El oferente debe incluir el licenciamiento, software y hardware requerido para el cumplimiento de lo solicitado por la entidad.

1.2. Clasificación UNSPC

SEGMENTO	FAMILIA	CLASE	PRODUCTOS	PRODUCTO
81	11	18	00	SERVICIO DE SISTEMAS Y ADMINISTRACIÓN DE COMPONENTES DE SISTEMAS
43	22	17	00	EQUIPO FIJO DE RED Y COMPONENTES
81	11	15	00	INGENIERIA DE SOFTWARE O HARDWARE
81	11	20	00	SERVICIOS DE DATOS
43	22	26	00	EQUIPO DE SERVICIO DE RED
81	11	22	00	MANTENIMIENTO Y SOPORTE DE SOFTWARE
81	11	17	00	SISTEMAS DE MANEJO DE INFORMACIÓN MIS
43	23	27	00	SOFTWARE DE APLICACIONES DE RED
43	23	28	00	SOFTWARE DE ADMINISTRACION DE REDES
43	22	25	00	EQUIPO DE SEGURIDAD EN RED
43	23	29	00	SOFTWARE PARA TRABAJO EN REDES
43	23	32	00	SOFTWARE DE SEGURIDAD Y PROTECCIÓN

2. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **DOS (2) MESES**, contados a partir de la suscripción del acta de inicio.

Nota 1: Las renovaciones son requeridas por **un periodo mínimo de diez (10) meses** en un esquema 7 x 24 ante fabricante y con las funcionalidades solicitadas de las plataformas para los equipos mencionados, garantizando las suscripciones de seguridad de los equipos durante el tiempo contratado e incluyendo acceso a soporte técnico de fábrica en esquema 7x24 y reemplazo de hardware (RMA) en caso de falla de este, para los elementos que aplique. El oferente debe incluir el licenciamiento, software y hardware requerido para el cumplimiento de lo solicitado por la entidad.

Nota 2: Lo anterior sin perjuicio de las obligaciones post-contractuales que se deriven de los servicios por concepto de soporte, período de vigencia del licenciamiento y demás obligaciones que requieran ejecutarse de forma posterior al plazo de ejecución contractual

3. DEFINICIONES

Adware: Software que se apoya en anuncios como parte del propio programa. La publicidad generada es mostrada después de la instalación de dicho programa.

Amenaza: Circunstancia que tiene el potencial de causar daños o pérdidas puede ser en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS).

Anti spam: Aplicación o herramienta informática que se encarga de detectar y eliminar correo no deseado.

Antivirus: Software utilizado para eliminar programas elaborados con intención destructiva.

Aplicación engañosa: Las aplicaciones engañosas pueden introducirse sigilosamente en su equipo cuando navega por la Web. Una vez instaladas, los estafadores las utilizan para cometer fraudes y robos de identidad.

Autenticación básica: Esquema de autenticación basado en la web más simple que funciona mediante el envío del nombre de usuario y contraseña con cada solicitud.

Ataque Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Ataque Dirigido: Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas.

Armouring: Es una técnica que utilizan los virus para esconderse e impedir ser detectados por los antivirus.

Blacklist (Lista negra): Es un proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bots (Red): Son grupos de ordenadores infectados controlados de forma remota por un hacker.

Bulo: Mensaje de correo electrónico con contenido falso o engañoso, pero con contenido de alto impacto.

Caballo de Troya: Son un tipo de código malicioso que parece ser algo que no es. Permiten hacerse con el control de los ordenadores ajenos sin permiso de los usuarios. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente.

Backup: Copia de seguridad. Esta se realiza para prevenir una posible pérdida de información.

Byte: Es la unidad de información utilizada por los computadores.

Carga destructiva: Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.

Cracker: Personas que rompen algún sistema de seguridad, (Fines de lucro, protesta o desafío).

Crimeware: Software malicioso como los virus, troyanos, spyware y más.

Ciberseguridad: Condición caracterizada por un mínimo de riesgos y amenazas a la infraestructura tecnológica, los componentes lógicos de la información y las interacciones en el ciberespacio.

Cibercrimen: Actos delincuenciales en el ciberespacio donde el principal objetivo es cometer ilícitos contra individuos, organizaciones y empresas.

Ciberdelito: Operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Cifrado: Proceso de codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

Control de acceso a la red (Nac): Su principal objetivo es asegurar que todos los dispositivos que sean conectados a las redes corporativas cumplan con las políticas de seguridad establecidas para evitar amenazas.

Correo no deseado: cualquier comunicación que nos llega por cualquier medio no habiendo sido solicitada y que no era esperada por el usuario que la recibe.

Cookie: Archivos que se guardan en los equipos para que los sitios web recuerden determinados datos.

Cluster: Es la unidad de almacenamiento en el disco rígido.

Definición de virus: Procedimiento por medio del cual el antivirus actualiza su base de datos de definiciones de virus. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes.

Delito Informático: Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Desbordamiento del búfer: Se producen cuando un programa sobrescribe otras partes de la memoria del equipo para almacenar más datos de los permitidos, provocando errores o bloqueos.

Driver: Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc).

Dropper: Es un fichero ejecutable que contiene varios tipos de virus en su interior.

Economía Clandestina: La economía clandestina en línea es el mercado digital donde se compran y se venden bienes y servicios obtenidos a través de la ciberdelincuencia, con el fin de cometer delitos informáticos.

Encriptación: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Exploit: Un error en el software que representa una brecha de seguridad.

Extorsión: Para el presente anexo se entiende por extorsión el uso de Internet para amenazar o intimidar a un individuo, para conseguir u obtener dinero u otra cosa del mismo.
Extensión: Los ficheros se representan asignándoles un nombre y una extensión, separados entre sí por un punto: NOMBRE.EXTENSIÓN.

Filtración de datos: Divulgaciones que no están autorizadas que tratan de adquirir información confidencial y que pueden dar lugar a robos o fugas.

Firewall: Un componente de hardware o software diseñado para bloquear el acceso no autorizado.

Firma de Antivirus: Las bases de firmas de un antivirus son el conjunto de cadenas que posee para detectar distintos códigos maliciosos. Sus actualizaciones se producen cuando

el producto descarga nuevas firmas, que son incorporadas a su base para así poder detectar más amenazas.

Freeware: Es todo aquel software, legalmente distribuido, de forma gratuita.

Gigabyte GB: Es la unidad de medida de una memoria. 1 gigabyte = 1024 megabytes = 1.073.741.824 bytes

Gateway: Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas.

Greylisting o Lista Gris: Una lista gris o greylist es una técnica para el control de mensajes spam. Es un método de defensa que bloquea la mayoría del spam que se recibe en un servidor de correo.

Gusanos: Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios.

Hacker: Persona experta en tecnología dedicada a intervenir y /o realizar alteraciones técnicas con buenas o malas intenciones.

Hacking: Acceder de forma ilegal a datos almacenados en un ordenador o servidor.

Hardware: Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, disco duro, otros).

Memoria de acceso aleatorio RAM: Es el lugar donde el computador almacena datos que le permiten al procesador acceder rápidamente al sistema operativo, aplicaciones y datos en uso.

Metadatos: Son datos altamente estructurados que describen información, contenido, calidad, condición y más características de los datos.
HTTP (HyperText Transfer Protocol: Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador.

Ingeniería Social: Término que hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

Incidente Informático: Es la violación o amenaza que afectan la confidencialidad, disponibilidad y la integración como la continuidad de los servicios que son ofrecidos.

Inyección de código SQL: Técnica donde el atacante crea o altera comandos SQL, para exponer datos ocultos, sobrescribir los valiosos, o ejecutar comandos peligrosos en un equipo que hospeda bases de datos.

Índice de peligrosidad: Es un valor calculado que permite medir lo peligroso que puede llegar a ser un virus.

Infección: Es la acción que realizan los virus, consistente en introducirse en el ordenador o en áreas concretas de éste y en determinados ficheros.

IP (Internet Protocol) / TCP-IP: La IP es la dirección o código que identifica exclusivamente a cada uno de los ordenadores existentes.

Keylogger: Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Lista Blanca: Método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

Malware: Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, keyloggers, Botnets, Ransomware, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues.

Mecanismo de Propagación: Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Mutex: Técnica utilizada por algunos virus para controlar el acceso a recursos (programas u otros virus) y evitar que más de un proceso utilice el mismo recurso al mismo tiempo.

Negación de servicio (DoS): Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Nivel de Propagación: Se trata de un valor que indica cómo de rápido se puede extender o se ha extendido el virus por todo el mundo. Es usado para mirar la peligrosidad del mismo.

Nuke (ataque): Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado.

Parches: Programa que se encarga de hacer cambios en busca de la corrección de vulnerabilidades de seguridad.

Pharming: Redirigir el tráfico a un sitio web falso para capturar información confidencial de los usuarios.

Phishing: Técnica utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

Piratería: Infringir los derechos de autor para obtener ganancias financieras o distribuir sin permiso un trabajo que se está preparado para su distribución comercial.

Programa malicioso: También conocidos como malware que contienen virus, spyware y otros programas indeseados que se instalan sin consentimiento.

Protección Heurística: En el contexto de la protección antivirus, la heurística se compone de un conjunto de reglas que se emplean para detectar el comportamiento de los programas maliciosos sin necesidad de identificar de forma exclusiva a la amenaza específica, como es requerida por la detección clásica basada en firmas.

Redes punto a punto: son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Ransomware: Programa maligno que bloquea totalmente nuestro equipo y pide dinero a cambio de devolver el control.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque.

RMA: Son las siglas en inglés de Return Merchandise Authorization, es decir, la autorización de devolución de mercancía.

Robo de datos: Los robos de datos pueden producirse tanto dentro de la empresa (por ejemplo, a manos de un trabajador descontento) como mediante ataques de delincuentes desde el exterior.

Rootkits: Es un juego de herramientas (programas) que permiten acceder a los niveles administrativos de un ordenador o una red.

Scareware: Hacer creer a los usuarios que el equipo está infectado, para hacer comprar una aplicación falsa.

Sistema de detección de intrusos (IDS): Hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Sistema de prevención de intrusiones (IPS): Encargados de detectar y bloquear cualquier intento de intrusión, transmisión de códigos maliciosos, o amenazas a través de la red.

Software de seguridad fraudulento (rogue): Falsos programas de seguridad que no son realmente lo que dicen ser, sino que todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.

Spear phishing: Estafa por correo electrónico cuyo objetivo es acceso no autorizado a datos, se centra en organizaciones en busca de: robo de propiedad intelectual, datos financieros, secretos comerciales, otros.

Spyware: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas sin permiso de los usuarios.

Toolkit: Son programas de software que pueden usarse tanto por novatos como por expertos para facilitar el lanzamiento y distribución de ataques a computadoras en red.

Tracware: Es todo programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por Internet (páginas visitadas, banners que pulsa, etc.) y crea un perfil que utiliza con fines publicitarios.

Transición es la acción y efecto de pasar de un estado a otro distinto. El concepto implica un cambio en un modo de ser o estar. Por lo general se entiende como un proceso con una cierta extensión en el tiempo.

Variante: Es una versión modificada de un virus original, que puede infectar de forma similar o distinta y realizar las mismas acciones u otras.

Vector de ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

Virus: Programa de ordenador capaz de incrustarse en disco y replicarse repetidamente, sin el conocimiento o permiso del usuario.

Versión IP: Versión IPv4 / IPv6. El Protocoló de Internet versión 6, en inglés, Internet protocol versión 6 (IPv6), es una versión del Internet protocoló (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocolo versión 4 (IPv4).

Vulnerabilidad: Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

Zombie: Ordenadores infectados controlados de forma remota por los ciber delincuentes.

4. CARACTERÍSTICAS Y CONDICIONES TÉCNICAS

4.1. ASPECTOS GENERALES

Se requiere realizar la renovación del licenciamiento y actualizaciones de la plataforma de solución de monitoreo y analítica de disponibilidad y ciberseguridad fortimonitor, fortianalyzer y tipo Deceptor VM orientada a la cacería de Amenazas por medio de Señuelos o Decoys en la cual se encuentran equipos tecnológicos de logs, reportes y monitoreo de la experiencia digital fortinet, ubicados en nube y en el data center administrativo de TRANSMILENIO S.A. Dicha renovación incluye soporte y garantía por diez (10) meses a partir de la firma del acta de inicio, en los que se encontraran vigentes los acuerdos de licenciamiento, garantía, soporte y RMA como servicios poscontractuales e inherentes a la renovación, con esquema de soporte 7x24 con fabricante y soporte local por parte del Contratista. La condición técnica para la renovación deberá realizarse en las mismas condiciones del licenciamiento actual, igualmente los servicios de soporte técnico.

4.1.1 CARACTERÍSTICAS TECNICAS

La solución tipo Deceptor VM debe contar con mínimo las siguientes características
• Debe permitir la creación de trampas activas con un flujo de tráfico de red falso entre las trampas implementadas para confundir y desviar a los atacantes que monitorean el tráfico, asegurando que interactúen con las trampas implementadas.

• Debe realizar ejecución de investigaciones proactivas de los eventos correlacionados para detectar amenazas avanzadas desconocidas.
• Debe permitir hacer visualización completa del ataque
• La solución ofertada debe incorporar paquetes de tokens para las máquinas señuelo o VM decoy.
• La solución ofertada debe soportar las siguientes acciones mediante integración con la solución Perimetral de NGFW.

- Bloqueo.
- Cuarentena.
- Exportación de IOCs.

• La solución deberá proporcionar reportes que caractericen tanto la identificación de incidentes como ataques detectados en la red de la entidad. Estos reportes deben incluir:

- Severidad.
- Última Actividad.
- Tipo del evento.
- Información de direccionamiento del atacante.
- Información de credenciales de uso del atacante.
- Información de direccionamiento de la Victima.
- Tiempo de iniciación del ataque
- Puertos de ejecución del ataque
- Tipo de Ataque
- Información de passwords usados por el atacante.
- Línea del tiempo.
- PCAP del tráfico capturado por el Decoy.

• Debe estar en capacidad de hacer detección de reconocimientos de red que usen ping (ICMP)
• Debe contar con señuelos que simulen conectores a base de datos que usend ODBC.

Debe integrarse con el Firewall de Nueva Generación de la entidad, de manera que se pueda tener en este último un dashboard centralizado con la información general del dispositivo y los señuelos desplegados.
• Debe permitir exportar indicadores de compromiso (IOC) al menos en formato CSV para su uso por parte de plataformas externas.
• Debe permitir el despliegue de señuelos en activos reales para que dirijan al atacante a la solución de decepción de amenazas.
• Debe tener la capacidad de emular activos del tipo Gateway de VPN SSL.
• Debe tener la capacidad de emular activos con servicios SAMBA, SMB, SSH y HTTP/S habilitados.
• Debe tener la capacidad de definir una lista de Ips legítimas de la red para que no generen alertas cuando interactúen con los señuelos.
• Debe permitir visualizar en un mapa los señuelos desplegados.
• Debe tener al menos 4 capas de decepción, con la capacidad de crear los siguientes elementos falsos:
- Señuelos de infraestructura (Sistemas operativos, cámaras, impresoras, bases de datos, entre otros).

- Carnadas o servicios falsos que se ejecuten sobre los señuelos (servidores web, aplicaciones, entre otros).
- Tráfico de red falso para detectar ataques de tipo MitM o app spoofing, entre otros.
- Tokens o recursos falsos desplegados sobre los señuelos (credenciales, archivos, recursos compartidos, conexiones RDP, entre otros)
▪ Los tokens falsos creados no deben ser visibles para los usuarios de la entidad, únicamente para el atacante.
- Todos los elementos falsos se deben desplegar sin requerir instalar agentes sobre la infraestructura real de la entidad
• La solución se debe poder instalar como appliance virtual y cubrir los siguientes Hipervisores:
- VmWare
- KVM - Hyper-V
• Debe poder instalarse en infraestructura de nube pública, como mínimo en:
- AWS
- Azure
- Google Cloud Platform
• Debe escanear automáticamente la red haciendo uso de técnicas de escaneo pasivo y sugerir los elementos de decepción que se deben desplegar.
• Debe poder desplegar señuelos relacionados con equipos médicos.
- PACS
- DICOM
- SPACECOM
• La solución debe poder crear señuelos para ambientes OT (Tecnología Operacional) y para redes SCADA (PLC, HMI, Sensores IoT, entre otros).
• La solución, al desplegar un señuelo, debe permitir una interacción completa sobre el mismo. Esto con el fin de evitar que el atacante detecte que se trata de un señuelo.
• La solución debe ofrecer diferentes tipos de señuelos para desplegar y adicionalmente, debe permitir la creación de señuelos personalizados.

La solución debe soportar el marco de referencia MITRE para Sistemas de Control Industrial (MITRE ICS).

Debe estar en la capacidad de crear señuelos falsos de tipo:

- SAP
- ERP

La solución debe tener un motor de inteligencia que emple tecnicas Antireconocimiento y Anti-Exploit para hacer rastreo de atacantes y correlacion de campanas en tiempo real.

Los indicadores de compromiso generados por la solución se deben poder compartir con diferentes herramientas de seguridad de la entidad. Incluido el formato STIX/TAXII
• La solución se debe integrar como mínimos con los siguientes elementos:
- Sistema de NGDFW de la entidad - Sistema de control de acceso a la red (NAC)
- Herramienta de Sandbox - Solución SIEM
- Solución de respuesta automática (SOAR)

- Virus Total Threat Intelligence - Solución de detección y respuesta en el endpoint (EDR)
• Debe ofrecer una representación visual tipo mapa que muestre en tiempo real los ataques o señuelos que han sido tocados por el atacante.
• Debe poder desplegarse en un entorno fuera de línea, sin acceso a internet.

4.2 ACUERDOS DE NIVELES DE SERVICIO

El servicio de soporte deberá ser prestado en modalidad 7x24x365 de acuerdo con los tiempos establecidos según la criticidad de los incidentes, por diez (10) meses a partir de la firma del acta de inicio, en los que se encontraran vigentes los acuerdos de licenciamiento, garantía, soporte y RMA como servicios inherentes a la renovación y que se constituyen en obligaciones pos contractuales.

Los anteriores servicios son inherentes a la naturaleza del servicio renovado.

4.2.1 SOPORTE PRIMER NIVEL

Este soporte se atenderá por medio de los canales electrónicos (correo-mesa de ayuda) o telefónicos dispuestos para tal fin, donde se canalizarán todas las solicitudes de servicio de los usuarios.

El ingeniero de servicio Nivel 1, documentará el caso y generará un número de *ticket* de seguimiento.

Desde el momento en el que sea reportada alguna falla, el contratista deberá efectuar el seguimiento y documentación a la misma, hasta que dicha falla haya sido superada totalmente, en este momento se validará la indisponibilidad del servicio, información que sirve de soporte para el respectivo descuento de facturación definido contractualmente. En caso de presentarse dicha indisponibilidad, se deberá cotejar con el interventor del contrato para evitar inconsistencias en la facturación del servicio.

4.2.2 SOPORTE SEGUNDO NIVEL

Una vez hechos los descartes en el Nivel 1 de soporte, si se determina la necesidad de hacer una valoración de la falla en sitio, se escalará el incidente al Nivel 2 de soporte, de manera que el personal designado estará disponible para desplazarse a los lugares donde se reporte la falla, y hacer los respectivos *check list* de falla y tomar las acciones necesarias para el restablecimiento de la operación, en función de la herramienta del incidente reportado.

Todo el proceso de atención, diagnóstico, seguimiento y herramienta del incidente quedará documentado en el Ticket abierto.

4.2.3 SOPORTE TERCER NIVEL

Este nivel está considerado para el escalamiento de problemas que, por su naturaleza y complejidad, requieren de la atención directa de personal especializado o fabricante, ya sea con la intervención directa de personal de manera remota o en sitio dependiendo de las características de las fallas.

ACTIVIDAD	DESCRIPCIÓN	TIEMPO DE RESPUESTA	TIEMPO DE RESPUESTA
Reporte de fallas	Evento que afecta el funcionamiento de la herramienta de manera total.	El ingeniero que recibe la solicitud de servicio contará con máximo 30 minutos para informar por correo electrónico y/o telefónicamente la actividad a realizar para dar herramienta al problema y el tiempo estimado de herramienta del mismo, dependiendo de la severidad de la falla. Las fallas se clasifican en:	
		a. Bajo: Evento que no afecta el funcionamiento de herramienta	12 Horas
		b. Medio: Evento que afecta el funcionamiento de una o más funcionalidades de la herramienta	2 Horas
		c. Alto: Evento que afecta el funcionamiento de la totalidad de la herramienta.	1 Hora
Cambios	. Solicitud modificación de configuración o aplicación de cambios por actualización.	El ingeniero que recibe la solicitud de servicio contará con máximo 30 minutos para informar por correo electrónico y/o telefónicamente el horario en el cual se realizará el cambio solicitado. Esta hora será acordada con el cliente. se deben ejecutar rutinas que afecten el funcionamiento de la herramienta, dichos cambios deberán hacerse en el tiempo de la jornada laboral. 5 * 24 horas.	30 minutos

Penalizaciones por incumplimiento de los ANS: El incumplimiento de los ANS dará lugar a la aplicación de un descuento consolidado que se aplicará sobre el valor de la facturación mensual, previo análisis de las razones que lo motivaron para solicitar la aplicación de las acciones correctivas.

CUMPLIMIENTO DE ANS RESOLUCIÓN DE SOLICITUDES	DESCRIPCIÓN	% DE DESCUENTO
TIEMPOS DE RESPUESTA SOLICITUDES	PRIORIDAD ALTA	3 % DE DESCUENTO EN LA FACTURA POR EL INCUMPLIMIENTO EN LOS ANS.
	PRIORIDAD MEDIA	2 % DE DESCUENTO EN LA FACTURA POR EL INCUMPLIMIENTO EN LOS ANS.

Nota: Los ANS aplican únicamente para descuento durante los dos (2) meses del contrato contados a partir de la firma del acta de inicio, debido a que la solución surtirá durante este lapso los procesos de instalación, afinamiento, actualización, parametrización y/o migración de funcionalidades que pueden generar posible indisponibilidad de servicios.

El licenciamiento contratado incluye durante los 10 meses acceso a soporte técnico de fábrica en esquema 7x24 y reemplazo de hardware (RMA) en caso de falla de este para los elementos que aplique.

5. LUGAR DE EJECUCIÓN

El lugar de ejecución del contrato será en la Sede administrativa de Transmilenio S.A., ubicada en la ciudad de Bogotá D.C., en la Avenida El Dorado 69-76 Torre 1 piso 6 Dirección de TIC.

6. FORMA DE PAGO

El pago del contrato será realizado teniendo en cuenta lo siguiente:

- Primer pago correspondiente al 50% del valor total del contrato, al cargue del licenciamiento para los equipos de **Monitoreo de la Experiencia Digital FortiMonitor), Consola de Reportes y Logs FortiAnalizer,** así como validación del despliegue de los servicios en los equipos Fortinet en mención.

- Segundo pago correspondiente al 50% a la entrega del informe de servicio en el que se plasme un resumen de las actividades realizadas (actualización, soporte y mantenimiento, estabilidad de la infraestructura), problemas presentados, soluciones utilizadas y recomendaciones validado por el supervisor del contrato.

La factura deberá estar soportada por:

- Certificación del cumplimiento del (los) pago(s) de las obligaciones al sistema de seguridad social integral y parafiscales respecto de sus empleados en el periodo facturado.
- El pago se realizará dentro de los treinta (30) días hábiles siguientes a la presentación de la factura mensual y demás documentos antes descritos.
- El valor a pagar comprende todos los costos directos e indirectos y demás gastos e impuestos causables a cargo del CONTRATISTA.
- Para la realización del pago o abono en cuenta se deberá contar con el recibo a satisfacción del objeto y cumplimiento de las obligaciones contractuales mediante el informe de actividades por parte del CONTRATISTA debidamente cargado y aprobado en SECOP II por el Supervisor, con su respectivo informe de supervisión.

- El valor de la presente contratación será cancelado por TRANSMILENIO S.A., mediante transferencia electrónica en la CUENTA BANCARIA de la Red ACH designada por el CONTRATISTA. La modificación a la cuenta bancaria referenciada en el presente parágrafo no requerirá la expedición de contrato adicional, modificatorio u otro sí, sino la simple manifestación de ello por parte del contratista al supervisor y la Dirección Corporativa.

7. SUPERVISIÓN

La supervisión y control de la debida ejecución del objeto contractual será ejercida por el Profesional Especializado 06 - Seguridad de la Información de la Dirección de TIC o el funcionario a quien designe el ordenador del gasto.

8. OBLIGACIONES DE LAS PARTES

8.1. OBLIGACIONES GENERALES DEL CONTRATISTA

Para dar entrega a satisfacción de la herramienta requerida por TRANSMILENIO S.A., el CONTRATISTA deberá cumplir con las siguientes obligaciones generales:

1. Cumplir cabalmente con el objeto contractual, las obligaciones contractuales, el alcance del objeto y con cada uno de los servicios descritos en este documento.

2. Permitir la práctica de auditorías por parte de TRANSMILENIO S.A., o a quien el ente Gestor designe y de los diferentes órganos de control, de acuerdo con la Ley.

3. Garantizar el cubrimiento del 100% de los gastos que ocasione la ejecución del contrato.

4. Responder a las solicitudes de documentación e información que solicite TRANSMILENIO S.A.

5. Responder sin perjuicio de la respectiva garantía por la calidad de los servicios contratados.

6. Cumplir con los compromisos asumidos en la oferta.

7. Abstenerse de dar declaraciones o entregar información en redes sociales, medios de comunicación y/o a cualquier agente externo a TRANSMILENIO S.A; sin previa consulta y autorización de la Subgerencia de Comunicaciones y Atención al Usuario de TRANSMILENIO S.A.

8. Asistir a las reuniones de avance del contrato citadas por la Dirección de TIC´s de TRANSMILENIO S.A. y/o el supervisor del contrato en el marco de ejecución contractual.

9. Acatar las instrucciones que durante el desarrollo del contrato se le impartan por parte de TRANSMILENIO S.A a través del supervisor del contrato.

10. Asegurar que desde el día de la suscripción del Acta de inicio del Contrato y por un periodo de diez meses el personal y equipos disponibles cumplan los requerimientos mínimos exigidos, parala ejecución del soporte y garantía post contractual.

11. Proceder a efectuar el cambio, sin condicionamiento alguno, sobre su equipo de trabajo o personal cuando se genere un incumplimiento que amerite su retiro y así lo solicite TRANSMILENIO S.A.; el contratante estará indemne por cualquier reclamación que eventualmente llegare a efectuar el trabajador, por lo cual el contratista hará personal y directamente las gestiones necesarias para este efecto.

12. Velar por el cuidado de la marca de TRANSMILENIO S.A, del Sistema TransMilenio y del SITP; en cada una de las acciones y sugerencias que imparta con motivo de la ejecución del contrato.

13. Gestionar y/o tramitar los permisos y demás acciones necesarias para el cumplimiento del contrato, así como, garantizar el cumplimiento de todos los requisitos legales para el desarrollo de cada una de las actividades. En cada caso el costo de los trámites y permisos que se requieran serán de exclusiva responsabilidad del contratista.

14. Abstenerse de usar los archivos generados y usados para distribución propia y/o comercial, por cuanto reconoce que son de propiedad exclusiva de TRANSMILENIO S.A., razón por la cual se debe firmar el acuerdo de confidencialidad correspondiente.

15. Realizar junto con TRANSMILENIO S.A. la liquidación del contrato una vez terminada su ejecución.

16. Las demás derivadas de la naturaleza del contrato a adjudicar.

8.2. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

Para prestar el servicio requerido por TRANSMILENIO S.A., el CONTRATISTA deberá cumplir con las siguientes obligaciones específicas:

1. Realizar la planeación de las obligaciones contractuales y pos contractuales, para lo cual se entregará un cronograma de actividades con los respectivos tiempos de entrega de renovaciones y posterior servicio de soporte y garantía.

2. Suministrar y garantizar la disponibilidad del personal mínimo de trabajo cumpliendo con los perfiles solicitados, y en caso de algún cambio se debe solicitar ante el supervisor del contrato, siempre y cuando se cumpla con los perfiles

mínimos requeridos, para las actividades requeridas tanto en el plazo de ejecución como el soporte y garantía pos-adquisición.

3. Dar estricto cumplimiento con todas las fases del contrato y obligaciones señaladas y necesarias para la ejecución del proyecto.

4. Asistir y participar en las reuniones, comités y demás convocatorias realizadas por el supervisor del contrato a fin de discutir los avances, hallazgos, inconvenientes, entre otros temas relevantes relacionados con el objeto y obligaciones del contrato contractuales y post contractuales. En estas reuniones se deberá contar con la presencia del líder del proyecto y las demás personas que solicite el supervisor.

5. Entregar al supervisor un informe detallado de cada fase de cumplimiento del objeto y avance del mismo.

6. Cumplir el desarrollo del contrato dentro de los horarios establecidos por el contratante.

7. Al finalizar cada visita correctiva y/o preventiva el contratista deberá:

- Generar un informe de servicio en el que se realice un resumen de las actividades efectuadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.

- Consignar en la misma acta o informe de servicio si hubo cambio de software y/o modificaciones en la configuración.

8. Realizar todas las actividades de instalación, implementación, configuración y puesta en marcha de las renovaciones ofertadas.

9. Incluir en el servicio de soporte la atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario hábil y no hábil durante desde el día de la suscripción del Acta de inicio del Contrato y por un periodo de diez meses donde se incluye servicios de soporte y garantía post contractual.

10. Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante y por un periodo de diez meses donde se incluye servicios de soporte y garantía post contractual.

11. Presentar previo a la firma del acta de inicio la certificación vigente en ISO/IEC 27001:2013 y/o ISO/IEC 27001:2022, con servicios integrados de análisis y gestión de incidentes y eventos de ciberseguridad y/o diseño, suministro, implementación, soporte, y mantenimiento de soluciones y servicios de seguridad de la información, conectividad y optimización para redes de nueva generación y/o servicios y soluciones de ciberseguridad, gobierno y outsourcing de tecnologías de información y/o monitoreo de eventos e incidentes de seguridad NOC-SOC y/o servicios SOC para prevenir y mitigar incidentes de ciberseguridad a través de procesos de identificación e investigación, cubiertos por el alcance de la certificación.

    Nota: En caso de presentarse una unión temporal la certificación de ISO/IEC 27001:2013 y/o ISO/IEC 27001:2022 podrá ser acreditada por una de las empresas que conforman la unión temporal.

12. Realizar durante la vigencia del contrato y por un periodo de diez meses donde se incluye servicios de soporte y garantía post contractual, dos (2) visitas en las cuales debe llevar a cabo actividades como Verificación y afinamiento de las plataformas, depuración de reglas, ajustes de configuración y demás actividades que se requieran para mantener los dispositivos afinados en procura de lograr la mayor efectividad posible para mitigar amenazas cibernéticas.

13. Guardar reserva sobre la información que adquiera en el desarrollo del contrato.

14. Recibir como mínimo una visita de auditoría y seguimiento por parte de TRANSMILENIO S.A., a las instalaciones de la empresa del contratista, para validar aspectos generales de seguridad de la información en lineamiento con las políticas vigentes en la materia al interior de TRANSMILENIO S.A.

15. Dar estricto cumplimiento de la Circular TMSA 009 de 2021, frente a la aplicación del Decreto Distrital 332 del 29 de diciembre del 2020 mediante el cual se incorpora medidas afirmativas que promuevan la participación de las mujeres en la ejecución de los negocios celebrado por el Distrito Capital. Para lo cual deberá incluir la respectiva certificación mensual por parte del revisor fiscal, indicando de forma detallada y expresa su cumplimiento porcentual. Sin perjuicio de lo anterior, la Entidad podrá requerir los soportes o información adicional que estime convenientes para verificar el cumplimiento de esta obligación contractual.

16. Las demás que tiendan al estricto cumplimiento del contrato, las consagradas en la ley y en los documentos que forman parte integral de este presente contrato.

8.3. OBLIGACIONES AMBIENTALES A CARGO DEL CONTRATISTA

De acuerdo con la Resolución 3179 de 2023 de la Secretaría Distrital de Ambiente " Por la cual se adopta la guía técnica para la formulación del Plan Institucional de Gestión Ambiental (PIGA), y se dictan lineamientos para su concertación, implementación, evaluación, control y seguimiento, y otras disposiciones", el Programa de Consumo sostenible debe evidenciar acciones que propendan por la implementación de lineamientos ambientales que promuevan el uso y consumo responsable de materiales, elementos, maquinaria, equipos o cualquier tipo de contratación que realice la entidad, mediante la asignación de obligaciones de orden ambiental y así hacer extensiva la cultura de gestión ambiental y responsabilidad social para lo cual deberá:

- Presentar un informe a la firma del Acta de Inicio, con la identificación de los residuos sólidos y residuos peligrosos que se pueden generar en el desarrollo del contrato y las correspondientes actividades generadoras.

- Realizar el manejo, recolección, transporte, tratamiento y disposición final de los residuos peligrosos generados en la ejecución del contrato conforme a lo establecido en la normatividad ambiental vigente.

- Realizar la gestión de los escombros generados en la ejecución del contrato, de acuerdo con lo contenido en el Decreto 1713 de 2002, Decreto 357 de 1997, Decreto 507 de 2023 y las normas que les modifiquen, adicionen y a aquella que surja en relación con el tema y sea aplicable durante la ejecución del contrato. Adjuntar copia de los correspondientes certificados de recolección y disposición.

- Presentar un informe mensual en el que incluya las cantidades y actividades generadoras de residuos sólidos y residuos peligrosos y escombros durante la ejecución del contrato y describa las actividades desarrolladas para la gestión de esos residuos de conformidad con la normatividad vigente aplicable y adjuntar copia de los correspondientes certificados que soporten la gestión dada.

- Capacitar periódicamente al personal, como mínimo una (1) vez cada trimestre del año, en gestión ambiental, gestión (manejo, disposición, recuperación y almacenamiento) de residuos sólidos y residuos peligrosos, así como en el manejo seguro de sustancias químicas. Adjuntar copia de los soportes de capacitación.

- Verificar periódicamente el estado de licencias y permisos de orden ambiental de las empresas gestoras de residuos peligrosos con las cuales se dispondrán los residuos generados por ejecución contractual.

- Dar cumplimiento a la normatividad ambiental vigente que por el objeto del contrato le sea aplicable y a aquella que surja en relación con el tema durante la ejecución

del contrato, principalmente lo concerniente a la gestión de residuos sólidos y residuos peligrosos.

- Cumplir con los requisitos de seguridad y salud ocupacional exigidos por las normas vigentes.

9. TRANSPORTE Y COMUNICACIONES

El transporte de los equipos objeto de la presente contratación estará a cargo del oferente y se entregaran en la sede administrativa de Transmilenio S.A., Avenida El Dorado 69-76 Torre 1 piso 6 Dirección de TIC.

10. EQUIPO MÍNIMO REQUERIDO

10.1. LÍDER DEL PROYECTO: Se deberá designar una única persona de contacto con quien TRANSMILENIO S.A., podrá efectuar el seguimiento a todas las obligaciones y responsabilidades del contrato.

ITEM	PERFIL	EXPERIENCIA CERTIFICABLE	TITULO DE POSGRADO	CERTIFICACIONES
LIDER DE PROYECTO	INGENIERO DE SISTEMAS Y/O INGENIERO DE TELECOMUNICACIONES Y/O INGENIERO ELECTRONICO Y/O INGENIERO TELEMÁTICO Y AFINES	MINIMO (5) CINCO AÑOS DE EXPERIENCIA PROFESIONAL.	GESTION Y/O GERENCIA DE PROYECTOS Y/O ADMINISTRACION DE PROYECTOS Y/O SEGURIDAD DE REDES TELEMÁTICAS	Deberá acreditar una o varias de las siguientes certificaciones: CERTIFICADO IPV6 SILVER Y/O GOLD IPV6 FORUM CERTIFIED PROFESSIONAL SECURITY OPERATIONS CERTIFICACION EN TECNOLOGIAS DECEPTOR Y/O EQUIVALENTES Y/O CERTIFIED SOLUTION SPECIALIST SECURITY OPERATIONS CERTIFICACION ISO/IEC 27001:2022 (vigente)
CANTIDAD	**1**			

NOTA: Las hojas de vidas del recurso humano deberán presentarse por el proponente adjudicatario previo a la firma del acta de Inicio, para la presentación en el proceso de

selección cada proponente deberá acreditar compromiso de presentación del personal bajo las condiciones establecidas en los documentos del proceso.

Deberá prestar sus servicios como mínimo durante periodo de ejecución del contrato resultante del presente proceso y el tiempo de garantía ofrecido por el proponente.

Los demás requisitos de este personal están establecidos en el estudio previo.

11. Área responsable de la adquisición
Aprobó: Director **Nombre: Rafael Felipe Valdez Laguado** **Dependencia: Dirección de Tecnologías de la Información y las Telecomunicaciones** **Revisó: Contratista Apoyo Técnico** **Nombre: Julian Andrés Rey Palencia** **Dependencia: Dirección de Tecnologías de la Información y de la Comunicación.** **Revisó: Contratista Apoyo Financiero** **Nombre: Dayanna Marisol Rodriguez Castro** **Dependencia: Dirección de Tecnologías de la Información y de la Comunicación.** **Revisó: Abogada Contratista Apoyo Jurídico** **Nombre: Isabel Cristina Cruz Moya** **Dependencia: Dirección de Tecnologías de la Información y de la Comunicación**
Fecha de elaboración del estudio (06/09/2024)**:**