1. OBJETO

DTC96 Contratar la renovación del licenciamiento, soporte y configuración de herramientas de punto final (End Point detection & response) TRAPS (Cortex) y/o sistemas integrados de seguridad perimetral FORTINET.

1.1. Alcance del Objeto

Se requiere renovar el esquema de licenciamiento y el soporte de la herramienta de punto final Cortex, para lo cual se requiere:

- Renovar el licenciamiento Cortex para 750 agentes.

- Las renovaciones son requeridas por un periodo de un (1) año en un esquema 7 x 24 ante fabricante de conformidad con lo establecido en el numeral 4.1.1 del documento anexo técnico (*4.1.1 CONDICIONES TECNICAS GENERALES DE LA RENOVACION CORTEX)* de la herramienta para el número de agentes requerido de setecientos cincuenta (750), garantizando las actualizaciones de seguridad de la herramienta durante el tiempo contratado.

- Acceso a soporte técnico de fábrica en esquema 7x24 Tipo Premium.

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 APLICAICONES DE RED
43	23	28	00	SOFTWARE DE ADMINISTRACION DE REDES
43	22	25	00	EQUIPO DE SEGURIDAD EN RED
43	23	26	00	SOFTWARE ESPECIFICO PARA LA INDUSTRIA
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 doce (12) Meses, contados a partir de la suscripción del acta de inicio. Teniendo en cuenta la configuración y estabilización del servicio y su puesta en marcha.

Nota 1: El tiempo de implementación y puesta en funcionamiento del esquema de servicios es inmediato contado a partir de la firma del acta de inicio, por parte de los representantes o delegados de las partes.

3. DEFINICIONES

Agente: Dispositivo informático que se comunica a través de una red a la que está conectado. Normalmente se refiere a los dispositivos que utilizamos a diario como ordenadores de escritorio, portátiles, teléfonos inteligentes, tablets o dispositivos de Internet.

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).

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.

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.

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

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.

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

Córtex XDR: Herramienta de Palo Alto Networks especializada en la detección de amenazas con precisión mediante análisis de comportamiento, además que permite revelar la causa original de cada incidente para acelerar las investigaciones

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 de 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.

DLL (Dynamic Link Library): traducidas al castellano como Bibliotecas de Enlaces Dinámicos, una DLL se compone en una sucesión de archivos compuestos por un ejecutable, que hacen posible la práctica de un proceso

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.).

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

Endpoint (punto final): En términos de herramientas de seguridad informática hace referencia a la práctica de proteger las redes empresariales contra las amenazas que se originan en los dispositivos remotos o locales.

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.

Fibra óptica: Es un medio de transmisión por medio del cual se envían pulsos de luz que representan los datos a transmitir.

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.

MD5 (Message-Digest Algorithm 5): En criptografía, MD5 (abreviatura de, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. Uno de sus usos es el de comprobar que algún archivo no haya sido modificado.

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.

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.

Proxy: Un servidor proxy proporciona una puerta de enlace entre los usuarios e Internet. Es un servidor denominado “intermediario”, porque está entre los usuarios finales y las páginas web que visitan en línea.

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.

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.

Scripts: En informática, un script hace referencia a una secuencia de comandos o “guion” que indica al computador las instrucciones que debe realizar.

SHA-256 (Secure Hash Algorithm-256): Conocido como algoritmo de hash seguro de 256 bits, es utilizado en criptografía. Los algoritmos de hash criptográfico generan hashes irreversibles y únicos. Cuanto mayor sea la cantidad de hashes posibles, menor será la probabilidad de que dos valores creen el mismo hash.

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.

Slack: es una aplicación de mensajería para empresas que conecta a las personas con la información que necesitan.

Software de seguridad fraudulento (rogue): Falsos programas de seguridad que no son realmente lo que dicen ser. 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.

Syslog: es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

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.

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.

VM (Virtual Machine): Una máquina virtual (VM) es un entorno informático aislado que se crea mediante la extracción de recursos de una máquina física.

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

WildFire®: Solución de análisis de malware en la nube de Palo Alto Networks®, utiliza aprendizaje automático e inteligencia colectiva para prevenir las amenazas desconocidas de forma integrada, automatizar la protección de otros servicios y acelerar las investigaciones.

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

4. CARACTERÍSTICAS Y CONDICIONES TÉCNICAS

Se requiere realizar la renovación del licenciamiento y actualizaciones de la herramienta de punto final Cortex por un (1) año. Dicha renovación incluye soporte y garantía por doce (12) meses a partir de la firma del acta de inicio, en los que se encontraran vigentes los acuerdos de licenciamiento, garantía, soporte por parte del contratista, garantizando que el end point como servicios poscontractuales e inherentes a la renovación, con esquema de soporte tipo Premium 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. ACUERDOS DE NIVEL 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 doce (12) meses a partir de la firma del acta de inicio, en los que se encontraran vigentes los acuerdos de licenciamiento, garantía, soporte y servicios inherentes a la renovación y que se constituyen en obligaciones poscrontractuales.

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

4.1.1 CONDICIONES TECNICAS GENERALES DE LA RENOVACION CORTEX

La renovación del licenciamiento deberá permitir:

- Inteligencia de amenazas WildFire
- Protección granular de los procesos secundarios
- Protección del ransomware basada en el comportamiento
- Escaneos periódicos para detectar malware inactivo
- Protección previa de exploits
- Prevención de exploits basada en las técnicas
- Prevención de exploits de kernels (núcleos

Adicional deberá contar con capacidades de detección y respuesta extendida

- Aislamiento de endpoint comprometido
- Terminal remota con ejecución de scripts, incluso si el OS no cuenta con phyton poder ejecutar un script
- Debe mostrar un análisis de remediación
- Analítica de punto final, que incluye identidad
- Recolección de datos de EDR de manera continua en la nube se detecte o no detecte actividad maliciosa
- Recolección de alertas de otras fuentes ajenas a los agentes de punto final
- Integración con virus total y otras fuentes de inteligencia de amenaza
- Reenvío de notificaciones vía syslog o Slack

- Capacidad de despliegue de un vm para hacer de proxy de las comunicaciones entre los agentes y su consola cloud en caso de que los agentes no tengan salida directa a internet.
- Capacidad de ejecutar scripts masivos en equipos que cuenten con la solución

Captura de datos en el endpoint

- El producto deberá de poder capturar, como mínimo, las siguientes acciones a nivel del endpoint en sistemas operativos Windows:
  - Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.
  - Actividades de creación, escritura, renombre, eliminación, modificación y creación de enlaces simbólicos de un archivo.
  - Se deberán de registrar los siguientes parámetros cuando sean cargados archivos DLL: ruta completa, dirección base, id del proceso o hilo que lo está cargando, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL, tamaño del archivo, tiempo de acceso del archivo.
  - Creación y terminación de los procesos
  - Inyecciones en hilos de procesos. ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto).
  - Las siguientes acciones de red: accept, connect, create, listen, close, bind, con los siguientes parámetros: IP y puerto destino, IP y puerto fuente, conexiones fallidas, protocolo (TCP/UDP), resolver los nombres de computadoras dentro de la red local.
  - Protocolos de red: peticiones DNS y respuestas UDP, HTTP connect, HTTP disconnect, HTTP proxy parsing.
  - Estadísticas de red. Volúmen al momento de ser enviado a través de un enlace TCP. Volúmen recibido a través de un enlace TCP.
  - Registro. Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardar llaves del registro
  - Sesiones del sistema operativo. inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.
  - Estado de la computadora: inicio, suspendida, reinicio. Con los siguientes atributos: nombre de la computadora, versión del sistema operativo, dominio, estado anterior y actual.
  - Logs de eventos de windows

4.2. SOPORTE PRIMER NIVEL

El soporte de primer nivel es el primer punto de contacto para los usuarios que necesitan asistencia técnica o resolución de problemas con el producto o servicio. A continuación, se explica sus características y funciones:

1. Primer punto de contacto: El soporte de primer nivel es el primer punto de contacto para los usuarios que necesitan asistencia.

2. Resolución de problemas básicos: Se enfoca en resolver problemas básicos y comunes que no requieren conocimientos técnicos avanzados.

3. Nivel de especialización: Los agentes de soporte de primer nivel tienen un nivel de especialización básico en el producto o servicio.

Funciones del soporte de primer nivel:

1. Recepción de solicitudes: Recibir solicitudes de asistencia de los usuarios.

2. Resolución de problemas: Resolver problemas básicos y comunes de manera eficiente.

3. Escalación de problemas: Escalar problemas complejos a niveles superiores de soporte cuando sea necesario.

4. Proporcionar información: Proporcionar información básica sobre el producto o servicio.

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 supervisor del contrato para evitar inconsistencias en la facturación del servicio.

4.2.1 SOPORTE SEGUNDO NIVEL

El soporte de segundo nivel es el siguiente nivel de asistencia técnica después del soporte de primer nivel. A continuación, se explica sus características y funciones:

Características del soporte de segundo nivel

1. Nivel de especialización: Los agentes de soporte de segundo nivel tienen un nivel de especialización más avanzado que los de primer nivel.

2. Resolución de problemas complejos: Se enfocan en resolver problemas más complejos que no pueden ser resueltos por el soporte de primer nivel.

3. Conocimientos técnicos avanzados: Los agentes de soporte de segundo nivel tienen conocimientos técnicos avanzados sobre el producto o servicio.

Funciones del soporte de segundo nivel

1. Resolución de problemas complejos: Resolver problemas complejos que requieren conocimientos técnicos avanzados.

2. Análisis y diagnóstico: Analizar y diagnosticar problemas para determinar la causa raíz.

3. Desarrollo de soluciones: Desarrollar soluciones personalizadas para problemas complejos.

4. Colaboración con otros equipos: Colaborar con otros equipos, como desarrollo o ingeniería, para resolver problemas complejos.

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.

4.2.2 SOPORTE TERCER NIVEL

El soporte de tercer nivel es el nivel más avanzado de asistencia técnica en una organización. A continuación, se explica sus características y funciones:

Características del soporte de tercer nivel

1. Nivel de especialización: Los agentes de soporte de tercer nivel tienen un nivel de especialización extremadamente avanzado y profundo en áreas específicas.

2. Resolución de problemas críticos: Se enfocan en resolver problemas críticos y complejos que no pueden ser resueltos por los niveles anteriores.

3. Conocimientos técnicos expertos: Los agentes de soporte de tercer nivel tienen conocimientos técnicos expertos y una comprensión profunda de la tecnología y los sistemas.

Funciones del soporte de tercer nivel

1. Resolución de problemas críticos: Resolver problemas críticos y complejos que requieren conocimientos técnicos avanzados y especializados.

2. Análisis y diagnóstico avanzado: Realizar análisis y diagnósticos avanzados para determinar la causa raíz de los problemas.

3. Desarrollo de soluciones personalizadas: Desarrollar soluciones personalizadas y complejas para problemas críticos.

4. Colaboración con otros equipos: Colaborar con otros equipos, como desarrollo o ingeniería, para resolver problemas complejos y críticos.

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.

Los siguientes son los acuerdos de niveles de servicio requeridos para la prestación del servicio de mantenimiento, en cumplimiento del objeto contractual y que estarán disponibles en los horarios establecidos en el presente documento.

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 solución al problema y el tiempo estimado de la misma, 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. Si 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

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 (12) 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 12 meses acceso a soporte técnico de fábrica en esquema 7x24.

4.2.3 Interrupción y ampliación de ANS

Los ANS serán interrumpidos y/o ampliados en las siguientes situaciones:

- Cuando los incidentes reportados por parte de TRANSMILENIO mediante los canales oficiales destinados para tal fin requieren mayor especificación y/o evidencia o no pueden ser complementados o verificados por el proveedor mediante el diagnóstico inicial, impidiendo así la solución definitiva de la incidencia por parte del contratista se debe registrar la novedad en el software que soporta el funcionamiento de la mesa de ayuda o en el sistema que haga sus veces y de esta manera se interrumpirán los ANS hasta que por parte de TRANSMILENIO se aporten los insumos faltantes. De no registrarse la novedad y no tener las evidencias correspondientes, no aplicara interrupción de ANS.

- Aquellos incidentes que pasen al fabricante o estén en adquisición de partes y el tiempo de solución acordado no es suficiente, por parte del contratista se debe registrar la novedad y se debe soportar técnicamente el motivo de la extensión del tiempo inicial, el cual debe quedar registrado en el software que soporta el funcionamiento de la mesa de ayuda del contratista o el que haga sus veces. De no registrarse la novedad y no aportar los soportes necesarios, no aplicará ampliación de ANS.

- Aquellos incidentes en los que se dé solución definitiva por parte del contratista y queden en espera de revisión y aprobación por parte de TRANSMILENIO para su correspondiente retroalimentación.

- De común acuerdo con TRANSMILENIO, en casos excepcionales y con el aporte de la justificación y soportes correspondientes.

  Nota: Solo se aceptarán máximo de una (1) ampliación para el tiempo de solución definitiva, de no cumplirse el tiempo se activarán nuevamente los ANS.

4.2.4 El descuento no aplica, en las siguientes circunstancias:

- La salida o interrupción de los servicios por la realización de trabajos o actividades de mantenimiento, cambios, pruebas, modificaciones o mejoras, debidamente planeadas o programadas, cuya ejecución sea notificada a TRANSMILENIO S.A., con al menos 2 días hábiles de anticipación.

- Cuando el Contratista o TRANSMILENIO S.A. requieran realizar una prueba de un servicio instalado con anterioridad (previa autorización y consenso), aunque no se haya reportado falla. En este caso el contratista debe haber informado con un tiempo mínimo de 3 días hábiles de antelación la realización de la prueba.

- La interrupción del servicio por previa programación de ventanas de mantenimiento, informadas por TRANSMILENIO S.A. y autorizadas por éste.

- En caso de existencia de casos fortuitos atribuibles a terceros o razones ajenas a la voluntad del Contratista, deben quedar expresas por escrito, debidamente probadas, justificadas y aceptadas por TRANSMILENIO S.A, planteando las opciones de solución y los tiempos.

5. LUGAR DE EJECUCIÓN

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

6. FORMA DE PAGO

La forma de pago se llevará a cabo de acuerdo con lo siguiente:

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

- Primer pago correspondiente al 50% del valor total del contrato, a la entrega y cargue del licenciamiento para los 750 agentes CORTEX en igual número de máquinas de la Entidad.
- Segundo pago correspondiente al 50% a la entrega del informe de servicio donde se evidencie la carga del licenciamiento y la validación del correcto

funcionamiento de los agentes en la consola Cortex y recibo por parte de la entidad.

- 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 Contratista deberá acreditar el pago de los aportes establecidos en el Artículo 50 de la ley 789 de 2002 y demás normas que lo modifiquen, reglamentan o complementen, lo cual se hará mediante certificación expedida por el Revisor Fiscal o el Representante Legal sino tiene Revisor Fiscal (Cuando aplique).
- El pago se realizará dentro de los treinta (30) días hábiles siguientes a la presentación de la factura mensual acompañada del certificado de cumplimiento emitido por el (los) supervisor(es) del (los) contrato (s) y la(s) certificación(es) del cumplimiento del (los) pago(s) de las obligaciones al sistema de seguridad social integral y parafiscales.
- El valor a pagar comprende todos los costos directos e indirectos y demás gastos e impuestos causables a cargo del CONTRATISTA.

NOTA 1: el contratista deberá informarse de forma suficiente y amplia de la normatividad tributaria y los costos asociados en esta materia que incluyan los impuestos distritales y nacionales que deba asumir para el desarrollo de la orden de compra.

NOTA 2: los valores de impuestos se causarán de conformidad con las normas tributarias vigentes.

NOTA 3: es responsabilidad exclusiva del contratista, revisar, indagar y considerar dentro de los costos de la propuesta que presente, la totalidad de los impuestos y contribuciones adicionales que se aplican en el Distrito, los cuales serán a su cargo si llegare a ser adjudicatario. La Entidad no reconocerá ningún costo adicional por estos conceptos en favor del Contratista, es responsabilidad del contratista asumir los costos asociados y es su entera responsabilidad en el desequilibrio que pueda generarse en caso tal de algún costo no previsto

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 aprobado 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.

En cada pago se tendrá en cuenta el cumplimiento de los ANS acordados y de conformidad con los descuentos realizados en caso de presentarse incumplimiento como consecuencia de falta de servicio los cuales tendrán afectación directa al pago de la factura por el no cumplimiento de estos, conforme a los porcentajes establecidos en el numeral “4.2.4 ACUERDO DE NIVELES DE SERVICIO (ANS)”, de este documento.

Las facturas presentadas por el contratista deben contener:

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 y documentación de pago correspondientes por parte del CONTRATISTA debidamente cargados y aprobados en SECOP II por el Supervisor, con su respectivo informe de supervisión.

El Contratista está en la obligación de entregar al Supervisor del contrato, la factura electrónica correspondiente a los servicios prestados; junto con el certificado de aportes a seguridad social, parafiscales y demás documentación solicitada, con lo cual el Supervisor del contrato expedirá el certificado para el pago y realizará el trámite ante el Área Financiera de la Entidad.

El Contratista debe tener en cuenta que la Supervisión cuenta con al menos cinco (5) días hábiles para realizar la revisión y aprobación del producto entregado, por lo que debe prever este tiempo en su programación presupuestal.

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 funcionario que 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 proyecto citadas por 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 del supervisor del contrato.

10. Asegurar que desde el día de la suscripción del Acta de inicio del Contrato y hasta la terminación del mismo, su personal y equipos disponibles cumplan los requerimientos mínimos exigidos contractualmente.

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 el supervisor del contrato; 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. Garantizar la confidencialidad sobre todos los archivos generados y usados por el contratista los cuales son de propiedad exclusiva de TRANSMILENIO S.A., no podrán ser usados para distribución propia y/o comercial del contratista, 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 del proyecto, para lo cual se entregará un cronograma de actividades con los respectivos tiempos de entrega descritas en el anexo técnico.

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

3. Suministrar todas las herramientas necesarias a nivel de hardware y software, para que los profesionales puedan efectuar su trabajo de la mejor manera.

4. Dar estricto cumplimiento con todas las fases del proyecto y entregables señalados en el anexo de especificaciones técnicas detalladas, necesarias para la ejecución del proyecto.

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

6. Cumplir el desarrollo del Contrato dentro de los horarios establecidos por TRANSMILENIO S.A.

7. Al finalizar cada visita correctiva 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 implementación 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 la vigencia del contrato.

10. Realizar en un lapso de doce meses, dos (2) visitas en las cuales debe llevar a cabo actividades como Verificación y afinamiento de la plataforma y/o solución, 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.

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 gestión y mantenimiento para soluciones de conectividad 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 diseño, comercialización, implementación y soporte en servicios de tecnologías de la información y las comunicaciones y/o análisis y gestión de incidentes y eventos de ciberseguridad, 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. Guardar reserva sobre la información que adquiera en el desarrollo del contrato.

13. Cumplir con los niveles de acuerdo de servicios (ANS).

14. 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. Paro 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.

15. Las demás que la empresa Transmilenio S.A considere pertinentes y las que se deriven del 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, en caso de que aplique.
- 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, en caso de que aplique
- Realizar la gestión de los escombros generados en la ejecución del contrato, de acuerdo con lo contenido en el Decreto 2981 de 2013, Decreto 357 de 1997, Resolución 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, en caso de que aplique.

- Adjuntar copia de los correspondientes certificados de recolección y disposición, en caso de que aplique.
- 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, en caso de que aplique.
- 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, en caso de que aplique.
- 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, en caso de que aplique.
- 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, en caso de que aplique.
- Cumplir con los requisitos de seguridad y salud ocupacional exigidos por las normas vigentes, en caso de que aplique.

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. PERSONAL MÍNIMO REQUERIDO

El equipo de trabajo deberá contar con un líder de proyecto de acuerdo con el siguiente perfil:

ITEM	LIDER DE PROYECTO	EXPERIENCIA CERTIFICABLE	TITULO DE POSGRADO	CERTIFICACIONES
PERFIL	INGENIERO DE SISTEMAS Y/O INGENIERO DE TELECOMUNICACIONES Y/O INGENIERO ELECTRONICO Y/O INGENIERO TELEMÁTICO	MINIMO (5) CINCO AÑOS DE EXPERIENCIA PROFESIONAL.	GESTION Y/O GERENCIA DE PROYECTOS Y/O ADMINISTRACION DE PROYECTOS Y/O SEGURIDAD INFORMATICA.	CERTIFICADO IPV6 SILVER Y/O GOLD IPV6 FORUM.
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. MATERIALES, EQUIPOS Y HERRAMIENTA

El contratista deberá suministrar todos los materiales, equipos, y herramientas necesarias para la correcta instalación y las actividades de mantenimiento y/o soporte preventivo y correctivo del sistema e infraestructura objeto del presente contrato, garantizando que estos cumplen con los estándares de calidad y normativas aplicables. Todo material utilizado deberá ser nuevo y adecuado para el tipo de equipo a mantener.

12. CALIDAD Y GARANTÍA DE LOS MATERIALES / BIENES SUMINISTRADOS

El contratista deberá garantizar que todos los materiales y bienes suministrados para la instalación y mantenimiento del sistema e infraestructura objeto del presente contrato sean de la más alta calidad, cumpliendo con las especificaciones técnicas y estándares internacionales. Los materiales utilizados deberán ser nuevos, libres de defectos, y estar certificados por el fabricante para asegurar su correcta operación y compatibilidad con los equipos.

El contratista deberá proporcionar una garantía sobre los materiales y bienes suministrados, cubriendo defectos de fabricación o fallas en el desempeño durante el período de garantía estipulado. Cualquier material defectuoso deberá ser reemplazado por el contratista sin costo adicional para TRANSMILENIO S.A., garantizando la continuidad del servicio.

13. SEGURIDAD Y SEGURIDAD EN EL TRABAJO.

Será responsabilidad del CONTRATISTA el cumplimiento de la normatividad legal vigente en materia de SEGURIDAD Y SALUD EN EL TRABAJO durante la ejecución del contrato, garantizando la gestión de la salud y la seguridad de los trabajadores a su cargo y/o partes interesadas.

Cada dependencia deberá enviar al área de Seguridad y Salud en el Trabajo la documentación precontractual de los procesos que se celebrarán para que desde el área se den los lineamientos en materia de SST de acuerdo con la naturaleza del contrato a suscribir.

14. INFORMES Y REUNIONES DE SEGUIMIENTO TÉCNICO:

14.1 INFORME MENSUAL

El Contratista deberá presentar, hasta la finalización el contrato, un informe mensual con fecha de corte al último día calendario, a partir de la suscripción del acta de inicio. El informe deberá radicarse en la entidad contratante en formato físico y digital, durante los cinco (5) primeros días hábiles del mes siguiente a la fecha de corte, y deberá contener, como mínimo:

a. Resumen ejecutivo.
b. Actividades realizadas de acuerdo con los hitos del cronograma de ejecución contractual que correspondan al periodo del reporte.
c. Avances de las metas de instalación y operación.

d. Ejecución presupuestal, estado de legalizaciones y amortización del anticipo (hasta cuando aplique)
e. Gestión de riesgos del proyecto.

f. Capítulo de operación (desde cuando aplique): Reporte del Sistema de Gestión; Indicador de velocidad de transmisión de datos promedio y pico en la red de acceso e interconexión, por canal; Indicador de uso de ancho de banda y consumo de datos por canal; Indicadores agregados para toda la red de acceso e interconexión indicando consumo de datos total y uso de ancho de banda, tanto promedio, como pico; y PQRSD.

Durante el primer mes de ejecución del contrato, será establecido entre el contratista, la y la supervisión los temas adicionales que deberá contener los informes mensuales.

La supervisión deberá revisar el informe mensual, y tendrá hasta diez (10) días hábiles, contados a partir del recibo del informe, para efectuar las revisiones y emitir la aprobación respectiva. En el evento de encontrar inconsistencias o datos incompletos, requerirá al (los) contratista (es) para que lleven a cabo los ajustes correspondientes, lo cual deberá surtirse en un plazo máximo de 5 días hábiles. Si vencido este plazo, la supervisión no aprueba totalmente los documentos, se podrán aplicar sanciones al contratista hasta la aprobación total del respectivo documento.

Nota: La entidad, a través de la supervisión podrá requerir en cualquier momento, durante la ejecución del contrato, un informe específico sobre las actividades enmarcadas en desarrollo del proyecto, para lo cual el contratista del contrato tendrá cinco (5) días hábiles contados a partir del requerimiento.

14.2 INFORME FINAL

Al finalizar el proyecto, el contratista se obliga a entregar a la supervisión, un informe final que contenga la información consolidada de las fases del proyecto, información histórica sobre la ejecución del proyecto, las lecciones aprendidas, y las principales dificultades encontradas durante la ejecución del proyecto y las recomendaciones para mitigar las mismas. Esta entrega deberá efectuarse el último día hábil del mes en que termina la ejecución del contrato.

11. Área responsable de la adquisición
Aprobó: director **Nombre: Rafael Felipe Valdez Laguado** **Dependencia: Dirección de Tecnologías de la Información y las Telecomunicaciones** **Elaboró: Profesional Grado 06** **Nombre: Javier Alfonso Castañeda Parra** **Dependencia: Dirección de Tecnologías de la Información y de la Comunicación.** **Revisó: Contratista Apoyo Técnico** **Nombre: Germán Guerrero** **Dependencia: Dirección de Tecnologías de la Información y de la Comunicación.** **Revisó: Contratista Apoyo Financiero** **Nombre: Dayanna Marisol Rodríguez 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** **Revisó: Contratista apoyo técnico** **Nombre: Julian Andrés Rey Palencia** **Dependencia: Dirección de Tecnologías de la Información y de la Comunicación**
Fecha de elaboración del estudio (06/06/2025)**:**