CONTRATO N° 120 DE 2024

ADQUISICIÓN DE HARDWARE Y SOFTWARE PARA LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD INTEGRAL Y LA RED INALÁMBRICA DE LA LOTERÍA DE MEDELLÍN

JUST IN TIME SOLUTIONS TRADE S.A.S

Entre los suscritos, **LOTERÍA DE MEDELLÍN**, Empresa Industrial y Comercial del estado, del Orden Departamental, creada mediante Decreto Ordenanzal 0819 de marzo 4 de 1996 con NIT 890.980.058-1, representada legalmente por **OCTAVIO DE JESÚS DUQUE JIMÉNEZ**, identificado con la cédula de ciudadanía No. 70.690.867, obrando en calidad de Gerente, quien en adelante y para efectos de este contrato será **LA CONTRATANTE** y la sociedad **JUST IN TIME SOLUTIONS TRADE S.A.S.**, identificada con el NIT. 900.731.082-5, representada legalmente por el señor **CAMILO ANDRÉS BAHAMON GENE**, identificado con cédula de ciudadanía No. 80.086.806, quien en adelante se denominará **EL CONTRATISTA**, hemos convenido celebrar el presente contrato, previas las siguientes consideraciones: 1) Que la Lotería de Medellín, es titular del monopolio rentístico de los juegos de suerte y azar en Antioquia. Para ello opera y comercializa su producto principal la Lotería de Medellín. También otorga y supervisa la concesión de apuestas permanentes, y a través de la Sociedad de Capital Público Departamental concede las autorizaciones para los juegos promocionales y las rifas que se pretendan realizar en el territorio departamental. 2) La oficina de tecnologías de la información y comunicaciones es un área de apoyo cuyo objetivo es mantener un alto nivel de seguridad, confiabilidad, disponibilidad y capacidad de respuesta con las soluciones y los servicios de TIC, mediante la formulación y evaluación de proyectos de adaptación, desarrollo, actualización y convergencia tecnológica. 3) La era digital está acelerando enormemente el ritmo de las economías, creando nuevas formas de operar las organizaciones y de ofrecer más y mejores productos y servicios, por lo que solo sobrevivirán las empresas capaces de adaptarse a las necesidades del mercado y a las nuevas formas de consumo. Los Data Center son importantes para seguir siendo competitivos, debe permitir acceder rápidamente a los servicios, las aplicaciones y los recursos que exige el dinámico mercado actual, así como a los recursos que serán necesarios en el futuro. Además de salvaguardar el recurso más importante para una organización como lo es la información. 4) Lotería de Medellín, para cumplir con sus objetos misionales, requiere de una plataforma tecnológica que soporte todos los procesos asociados a las siguientes actividades:

- Operación y Venta de la Lotería de Medellín y sorteos extraordinarios.
- Vigilancia y control del contrato de la concesión del chance para Antioquia.
- Gestión de las actividades misionales de la Sociedad de Capital Público Departamental.
- Gestión Administrativa de la lotería.
- Incentivo de Premio Inmediato (IPI).

5) La Oficina de Tecnologías de la Información y las Comunicaciones tiene como finalidad que se suministre, se mantenga y se modernice la infraestructura informática que permita implementar juegos de suerte y azar en línea y agilizar los procesos estratégicos, de apoyo y de control de la empresa, en condiciones de eficiencia, eficacia y transparencia, de acuerdo con la normatividad, principios y buenas prácticas, respecto a su consecución, administración y suministro. 6) Uno de los principales pilares de la

infraestructura tecnológica de las organizaciones es la seguridad de su principal activo: la información. El Ministerio de Tecnologías de la Información y las comunicaciones de Colombia ha venido en los últimos años en Colombia intensificando sus lineamientos para las entidades públicas y privadas en materia de seguridad digital, y por ello uno de los componentes pilares del Formulario Único Reporte de Avances de la Gestión, FURAG, tiene hoy en día gran cantidad de ítem de evaluación en materia de seguridad digital. A través de la política de Gobierno digital, el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia ha desarrollado dos herramientas básicas en la cual las entidades encuentran lineamientos y buenas prácticas de cómo ajustar cada uno de los elementos en los procesos de planeación y gestión de la seguridad de la información.

- El Modelo de Seguridad y Privacidad de la Información (MSPI)
- El Modelo de Riesgos de Seguridad Digital - Guía para la Administración del Riesgo y diseño de controles para las entidades públicas (DAFP).

7) El MSPI imparte lineamientos a las entidades públicas para la adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información. Y el Modelo de Gestión de Riesgos de Seguridad Digital tiene por objetivo brindar un marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta al momento de llevar a cabo actividades socio económicas en el entorno digital (prestación de trámites, servicios internos y externos, transacciones en línea entre otros) para así, fomentar y mantener la confianza de las múltiples partes interesadas (proveedores, ciudadanos, entidades públicas y privadas) en el uso del entorno digital en su interacción con el Estado, impulsando así la prosperidad económica y social del país. 8) Una evaluación de INTERPOL sobre las repercusiones de la COVID-19 en la ciberdelincuencia ha puesto de manifiesto un cambio sustancial en los objetivos de los ataques, que antes eran particulares y pequeñas empresas y ahora tienden a ser grandes multinacionales, administraciones estatales e infraestructuras esenciales. 9) Hoy en día la lotería de Medellín posee su propio portal de venta electrónica, el cual fue potencializado durante la pandemia COVID 19 y se ubicó en la primera fuente de ingresos durante la emergencia sanitaria. Para el año 2023 el portal de venta electrónica transo más de 14 mil millones de pesos, un 29% más que en el año anterior. 10) Por ello y con el fin de salvaguardar la información, la lotería de Medellín debe proteger toda su plataforma tecnológica ante eventos inesperados en materia de seguridad de información.11) Actualmente la Lotería de Medellín no cuenta con un sistema de seguridad integral, si bien contamos con equipos de seguridad en el perímetro (firewall y firewall de la web) , no se encuentra integrado con elementos de seguridad en estaciones de trabajo o end point, y otros elementos de red y de servicios de internet que requieren protección especial y proactiva. 12) El sistema actual tiene más de 5 años de implementado y cuenta con contratos de soporte, mantenimiento y garantía hasta el próximo mes de noviembre (ver imagen) y en caso de materializarse un riesgo no podremos reaccionar rápidamente para continuar con la operación en caso de que se venzan el contrato actual de soporte. 13) Por todo lo anterior se requiere renovar la infraestructura en materia de seguridad perimetral y de usuario final con el fin de salvaguardar la información de la lotería de Medellín. 14) En el documento emitido en mayo del 2016 por Coljuegos, titulado *"Requerimientos técnicos de juegos operados por internet en Colombia"* en el capítulo V "*Seguridad del sistema*", manifiesta la importancia y da lineamientos sobre la seguridad para el sistema técnico de juego. 15) En tal sentido es muy importante la implementación de

un sistema de seguridad integral que permita mitigar las amenazas detectadas y que garanticen la operación del negocio. 16) Que para satisfacer esta necesidad la Lotería de Medellín dio apertura a la Invitación Pública No.002 del 2024, a través de la Resolución N° 223 del 9 de septiembre de 2024. 17) Que, una vez finalizado el proceso de selección, mediante Resolución No. 259 del 8 de octubre de 2024, se el adjudicó la ejecución del contrato a la sociedad **JUST IN TIME SOLUTIONS TRADE S.A.S.** 18) Que por lo dicho anteriormente existe la viabilidad financiera y jurídica para suscribir el presente contrato, el cual se regirá por las siguientes cláusulas. **CLÁUSULA PRIMERA. OBJETO.** Adquisición de Hardware y Software para la implementación del sistema de seguridad integral y la red inalámbrica de la Lotería de Medellín. El estudio de conveniencia, el pliego de condiciones, sus adendas y la propuesta presentada por EL CONTRATISTA hacen parte integral del contrato, en las condiciones que no sean contrarias a las cláusulas de este. **PARÁGRAFO PRIMERO. ALCANCE:** Renovación de 2 firewall de seguridad perimetral, 2 firewall de aplicaciones web, un analizador de eventos, 8 switches de comunicación de usuario final, sistema de identificación y defensa de fugas de datos en tiempo real de manera automática y eficiente para 500 dispositivos y renovación de soporte y mantenimiento para 21 accespoint (wifi) y para 2 switches core de servidores. Todo debidamente configurado y puesto en producción. **PARÁGRAFO SEGUNDO. ESPECIFICACIONES TÉCNICAS**: El contratista deberá entregar las siguientes soluciones, debidamente instaladas y configuradas con, mínimo, las políticas actuales de la lotería de Medellín, así:

ITEM	Características
2 FIREWALL FORTIGATE 400F Configurados en Alta Disponibilidad (HA)	**CAPACIDADES** - 16Gigas de Memoria RAM. - Trusted Platform Module (TPM): Yes: **INTERFACES Y MODULOS:** - 16 puertos RG45 de 1GE. - 4 puertos 1GE/10GE SFP+ slots. - 4 puertos 10GE SFP+ Ultra Low Latency Slots. - 8 puertos 1GE SFP slots. - 2 puertos GE RJ45 para Management. - 1 puerto USB. - Un puerto RJ45 Console. **CAPACIDADES DE PERFORMANCE DE SISTEMA** - IPS Throughput: 12 Gbps. - NGFW Throughput: 10 Gbps. - Threat Protection Throughput: 9 Gbps **CAPACIDADES DE PERFORMANCE DEL SISTEMA** - IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP): 79.5 / 78.5 / 70 Gbps - IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP): 79.5 / 78.5 / 70 Gbps - Firewall Latency (64 byte, UDP): 4.19 µs.

	- Firewall Throughput (Packet per Second): 105 Mpps - Concurrent Sessions (TCP): 7.8 Millones - New Sessions/Second (TCP): 500 000 - Firewall Policies: 10 000 - IPsec VPN Throughput (512 byte) 1: 55 Gbps - Gateway-to-Gateway IPsec VPN Tunnels: 2000 - Client-to-Gateway IPsec VPN Tunnels: 50 000 - SSL-VPN Throughput: 3.6 Gbps - Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode): 5000 - Application Control Throughput (HTTP 64K): 28 Gbps - Virtual Domains (Default / Maximum): 10 / 10 - máximo número de FortiSwitches Soportados para Gestión centralizada: 72 - Máximo número de FortiAPs soportados para gestión centralizada (Total / Tunnel): 512 / 256 - Máximo número de FortiTokens soportados: 5000 CERTIFICACIONES Y AMBIENTE DE OPERACIÓN - Operating Temperature :32°F to 104°F (0°C to 40°C) - Storage Temperature :-31°F to 158°F (-35°C to 70°C) - Humidity :5% to 90% non-condensing - Noise Level :LPA 48 dBA / LWA 55 dBA - Airflow :Side and Front to Back - Operating Altitude :Up to 10 000 ft (3048 m) - Compliance :FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
1 PLATAFORMA DE GESTION Y ANALISIS AVANZADO: FAZ-300G	CAPACIDAD Y PERFORMANCE - Soporte hasta 100 GB logs por dia. - Rata de analítica de logs sostenida: 2000 logs/segundo - Devices/VDOMs (Máximo soportados) :180 - Máximo número de días de analítica: 50 LICENCIAMIENTO Y CAPACIDADES DE SEGURIDAD INCLUIDOS Licenciamiento ENTERPRISE PROTECTION, EL CUAL INCLUYE las siguientes capacidades de seguridad: - FortiGuard Indicators of Compromise Service: El servicio de indicadores de compromiso FortiGuard proporciona a los equipos de seguridad datos forenses de 500 000 IOC por día, que se utilizan en combinación con el análisis de FortiAnalyzer para identificar usos sospechosos y artefactos

	observados en la red o en un sistema de operaciones, que se han determinado con gran confianza como infecciones o intrusiones maliciosas, y un nuevo análisis histórico de los registros para la búsqueda de amenazas. - **Security Automation Service:** La suscripción al Servicio de automatización de seguridad permite una mayor automatización de la respuesta a incidentes con monitoreo y escalamiento mejorados, flujos de trabajo de gestión de incidentes integrados, conectores, manuales y más. - **FortiGuard Outbreak Detection Service:** El servicio de detección de brotes FortiGuard ofrece la descarga automática de paquetes de contenido para detectar el malware más reciente, incluido un resumen de los brotes y un mapeo de la cadena de ataque para saber cómo funciona el malware. El paquete incluye un informe FortiGuard para el brote, un controlador de eventos y una plantilla de informe para detectar brotes. ESPECIFICACIONES DE HARDWARE - Form Factor (supports EIA/non- EIA standards) :1 RU Rackmount - Total Interfaces :4x RJ45 GE - Storage Capacity :8 TB (2x 4 TB) - Usable Storage (After RAID) :4 TB - Removable Hard Drives :No - RAID Levels Supported :RAID 0/1 - RAID Type :Software - Default RAID Level :1 - Redundant Hot Swap Power Supplies :Optional AMBIENTE DE OPERACION - AC Power Supply :100–240V AC, 60–50 Hz - Power Consumption (Average / Maximum) :90.1 W / 99 W - Heat Dissipation :337.8 BTU/h - Operating Temperature :32°F to 104° F (0°C to 40° C) - Storage Temperature :-13°F to 167° F (-25°C to 75° C) - Humidity :20% to 90% non-condensing - Forced Airflow :Front to Back - Operating Altitude :Up to 7400 ft (2250 m). Safety Certifications : FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST
2 FIREWALL DE APLICACIONES WEB FORTIWEB 400F	ESPECIFICACION DE HARDWARE: - 4 puertos de red de x1 (10/100/1000)GE RJ45. - 4 puertos de red x1GE SFP ports.

Configurados en Alta Disponibilidad (HA)	- 480 GB SSD storage. - Memoria RAM: 16Gigas. - USB Interfaces: 2 - Form Factor:1U - Power Supply: Single PERFORMANCE DE SISTEMA OFRECIDO: - Throughput: 500 Mbps - Latency: <5ms - High Availability:Active/Passive, Active/Active Clustering - Administrative Domains:32 AMBIENTE DE OPERACION: - Power Required:100–240V AC, 50–60 Hz - Corriente maxima:100V/1.53A, 240V/0.64A - Power Consumption (Average):127.33 W - Heat Dissipation:521.38 BTU/h - Operating Temperature:32°F to 104°F (0°C to 40°C) - Storage Temperature: -13°F to 158°F (-25°C to 75°C) - Forced Airflow:Front to Back - Humidity:5% to 95% non-condensing CERTIFICACIONES DE CUMPLIMIENTO: - Safety Certifications: FCC Class A Part 15, RCM, VCCI, CE, UL/CB/Cul LICENCIAMIENTO Y CAPACIDADES DE SEGURIDAD INCLUIDOS Se incluye licenciamiento ADVANCED BUNDLE, EL CUAL INCLUYE las siguientes capacidades de seguridad: - **Protección de aplicaciones web:** protección de múltiples capas contra los 10 principales ataques a aplicaciones de OWASP, incluido el aprendizaje automático para defenderse de ataques conocidos y desconocidos. - **Protección de API:** proteja sus API de actores maliciosos al aplicar automáticamente políticas de seguridad positivas y negativas. Integre sin problemas la seguridad de API en su canalización de CI/CD. - **Mitigación de BOTS:** FortiWeb protege contra bots automatizados, raspadores web, rastreadores, recolección de datos, robo de credenciales y otros ataques automatizados para proteger sus activos web, API móviles, aplicaciones, usuarios y datos confidenciales. Al combinar

	el aprendizaje automático con políticas como detección basada en umbrales, engaño de bots y detección basada en biometría con una identificación superior de bots, FortiWeb puede bloquear ataques de bots maliciosos y, al mismo tiempo, reducir la fricción con los usuarios legítimos. Con técnicas de seguimiento avanzadas, FortiWeb puede diferenciar entre humanos, solicitudes automatizadas e infractores reincidentes, rastrear el comportamiento a lo largo del tiempo para identificar mejor a los humanos de los bots y aplicar desafíos CAPTCHA cuando sea necesario. Junto con FortiView, el panel de análisis gráfico de FortiWeb, las organizaciones pueden identificar rápidamente los ataques y diferenciar entre bots buenos y usuarios legítimos.
8 SWITCHES FORTISWITCH448E	**GENERALIDADES:** - Debe soportar capacidades de enrutamiento Capa 3. - Numero de puertos: 48 x1GbE RJ45 Detección Automática (Auto Sensing) - PoE+ (803.at/af): Configurable y soportable en los 48 puertos. - Uplink: 4 Puertos 10GbE SFP + - Compatiblidad con transceivers LX (1G SM), SX(1 G MM), ZX (1G),SR(10G), LR(10G), ER(10G) - Cada Switch debe incluir puerto serial para administración: de consola RJ-45. - Cada Switch debe incluir puerto de gestión fuera de banda (Out-of-band Ethernet management) - Debe ser máximo de 1 Unidad de rack EIA estándar de 19 in. - Capacidad de Conmutación >= 176 Gbps - Capacidad de transmisión de Paquetes Throughput >=262 Mpps - latencia <= 1 Microseg - Consumo de potencia maximo 772W - Fuente de poder redundante: opcional - Garantía limitada de por vida (5 Años después de fin de venta) - Jumbo Frame - Ethernet / >=10KB - MAC address table size >= 32.000 - La solución switches de core y distribución ofertada debe ser de la misma marca de la solución de acceso inalámbrico y solución Seguridad perimetral y de aplicaciones de este proceso de contratación para garantizar el SD-LAN de la Entidad

	- Presupuesto de potencia PoE+ ofertado no deberá ser menor a 420W. FUNCIONES L2 (QUE EL DISPOSITIVO DEBE SOPORTAR) - Soportar RMON (RFC 2819), Sflow (RFC 3176). - EEE 802.1Q, VLAN Ids>= 4.000 , Soportar IEEE 802.1ad QinQ - Private Vlan - Soporte de agregación de enlaces L2 vía LACP mínimo 8, Al menos agregación de 16 enlaces por troncal. - Mínimo ACLs: 1500 - Instancias de spanning tree mínimo: 16 - Entrada de Host mínimo: 16000 - Soportar Cables virtuales (virtual Wire) entre puertos. - Debe soportar DHCPv6 Snooping, IPV6 RA guard, - Debe soportar captura de paquetes - Debe contar con al menos un medio de monitoreo o alerta de fallas en conexiones de cobre, y un medio de monitoreo o alerta de fallas en conexiones de fibra. Especificar la nomenclatura del fabricante de estos métodos tanto para conexiones de cobre como para conexiones de fibra. - STP Root Guard, STP (802,1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), RPVST (Rapid per Vlan Spanning Tree) - Debe soportar MCLAG (multichassis link aggregation) - Debe soportar Port Mirroring para la supervisión del tráfico de la red CALIDAD DEL SERVICIO - QoS que cumpla con: clasificación, marcado, policy, strict priority, WRED - Debe soportar QoS marking (IPv4/IPv6) - Debe soportar Egress priority Mapping (Ipv4/IPv6) - Packet buffer mínimo de 4MB - Debe soportar Notificacion de Congestion explicita (ECN) para IPv4 e IPv6 GESTION - Administración mediante consola para CLI (Command Line Interface). No se admiten equipos de línea small business: equipos cuya administración sea únicamente a través de http / https. - Administración: o Interfaz de línea de Comandos Estándar de la Industria. o SNMP V1/2c/3. o Soportar ACL IPV4/IPV6.

	o Administración de VLAN. o Soporte a Voice VLAN. o Soportar administración basada en SSH y telnet. o Soportar OpenFlow o Netconf o Rest Apis. o Soportar SFlow o Netflow. - Debe soportar Administracion desde Sistemas de Gestion en Nube o on-Premise - En caso de no contarse con el Controlador SD-LAN, este debe incluirse en la propuesta con todas las funcionalidades y sistema de Gestion necesarias para este proyecto. - Se debe poder administrar Switches, Access Point, SD-WAN y Firewalls desde la misma consola de Administración FUNCIONES L3 - Debe soportar RIP (IPV4/IPV6), VRRP (IPV4/IPV6) y OSPF (IPV4/IPV6). Debe soportar enrutamiento estático y dinámico - Soportar BGP (IPv4/IPv6) - Soportar ISIS (IPv4/IPv6) - Soportar BFD (IPv4/IPV6) - Soportar BFD para RipNG (IPV6) - Rutas IPV4 soportadas estáticas y dinámicas >= 1000 - Debe soportar DHCP-Server - Rutas IPV6 soportadas >= 500 SEGURIDAD - Debe estar en capacidad de detectar Dispositivos IoT - Debe soportar el movimiento de clientes de un puerto a otro sin necesidad de borrar la sesion 802.1X. - El switch debe permitir descargar políticas de seguridad desde el firewall perimetral de la Entidad - Debe permitir la autenticación y autorización Local RADIUS y TACACS+ - Debe soportar Port Mirroring para la supervisión del tráfico de la red - Debe soportar SSH - Debe soportar DHCP snooping, DHCPv6, IP source guard, Dynamic ARP - Soportar la configuracion de interfaces fisica para enrutamiento - Debe soportar IEEE 802.1X (Port Based Network Access Control) - Debe soportar PTP (IPV4 e IPv6) - Debe soportar FIPS-140-2 (Nivel 2)

	- Debe soportar una funcionalidad de ahorro de Energia que baje consumo si no hay tráfico y si llega tráfico hacia el PC se envie mensaje de enciendido (Wake-On-Lan - WOL) GARANTIAS - MTBF mínimo de 10 Años (87600 horas) - El equipo debe contar con Garantía Limitada de por Vida de mínimo 5 Años después de fin de venta. - Cumplimiento de normas FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 -
1 EDR – DISCOVERY, PROTECT AND RESPOND para 500 dispositivos	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)** GENERALIDADES - La solución de EDR debe proporcionar a la ORGANIZACIÓN un conjunto de protecciones, tanto en pre-ejecución (esto es, antes de que la amenaza tenga capacidad para comprometer sus sistemas) como post-ejecución (cuando la amenaza interactúa con el servidor o equipo de trabajo), 100% basado en comportamiento (sin firmas estáticas) y cuya velocidad de respuesta proporciona una protección en tiempo real a los sistemas. FUNCIONALIDADES DE PREVENCION - El EDR debe utilizar un motor antivirus de aprendizaje automático para detener la ejecución previa de malware. Esta capacidad NGAV viene integrada en un agente único y ligero, lo que permite a los usuarios asignar protección antimalware a cualquier grupo de terminales sin necesidad de ninguna solución adicional. - Disponer de aprendizaje automático, NGAV basado en kernel y Machine learning (ML) - Enriquecer los eventos de seguridad con información sobre amenazas en tiempo real desde una base de datos en la nube que se actualiza continuamente. - Proteger los endpoints desconectados de la red con una protección fuera de línea; este modo de operación se denomina modo autónomo. - Proporcionar un control de dispositivos USB basado en múltiples parámetros. - Debe estar en capacidad de eliminar tiempos de permanencia y Fatigas por exceso de alamas (falsos positivos)

	FUNCIONALIDADES DE DESCUBRIMIENTO - El EDR debe contar con un sistema automatizado de control de políticas de superficie de ataques, con evaluaciones y descubrimiento de vulnerabilidades que permiten al personal encargado de la seguridad - Descubrir y controlar dispositivos no autorizados (por ejemplo, dispositivos no protegidos o no administrados) y detectar dispositivos IoT. - Realizar un seguimiento de aplicaciones ejecutadas, y su clasificación de seguridad. - Descubrir y mitigar las vulnerabilidades del sistema y las aplicaciones con parches virtuales, mediante el análisis de sus comunicaciones e inhabilitando el acceso a su comunicacion con el exterior - Al descubrir las vulnerabilidades debe mostrar la clasificación de reputación y el detalle de los códigos CVE aplicables - Reducir la superficie de ataque con políticas proactivas basadas en niveles de riesgo. FUNCIONALIDADES DE DETECCION Y PROTECCION - El EDR debe detectar y desactivar el malware así sean amenazas del tipo sin archivos o file-less y otros ataques avanzados en tiempo real para proteger los datos y evitar brechas en la seguridad en la entidad. Tan pronto como el EDR detecte flujos y comportamientos sospechosos, inmediatamente debe desactivar las amenazas potenciales, bloquear las comunicaciones salientes y el acceso al sistema de archivos desde esos procesos sospechosos, por otro lado debe evitar la exfiltración de datos, las comunicaciones de comando y control (C&C), la manipulación de archivos y el cifrado de ransomware. Al mismo tiempo, el backend del EDR debe continuar recopilando evidencias adicionales, enriqueciendo los datos de eventos y clasificando los incidentes para aplicar de forma automatizada una estrategia de respuesta a Incidentes, permitiendo así automáticamente la continuidad del negocio incluso en dispositivos ya comprometidos cumpliendo como mínimo con los siguientes ítems: - Se debe basar en la detección integrada de forma profunda en el sistema operativo, permitiendo la detección de

	ataques de infiltración sigilosa, los ataques basados en la memoria y los ataques "living off the land". - Debe Proporcionar protección en los procesos en ejecución, el inicio y parada de procesos, y en las interacciones entre procesos, así como frente a actividades sospechosas asociadas a librerías (archivos DLL en el caso de sistemas operativos Windows). - Debe poder Detener las amenazas en tiempo real y eliminar el tiempo de permanencia de dichas amenazas en la organización, incluso en los endpoints desconectados de la red corporativa. - Debe Bloquear las comunicaciones de forma granular a nivel de proceso, evitando exfiltraciones de datos, movimientos laterales y conexión con redes de comando y control. - Debe Impedir a los procesos maliciosos el acceso a los sistemas de ficheros, protegiendo frente a cifrados de ransomware, y la creación/modificación/eliminación maliciosa de archivos y/o registros. - Debe Permitir definir listas blancas y negras para personalizar mediante exclusiones estas protecciones (por hash, nombre y/o ruta de archivo, o por aplicación, incluyendo datos de versión y fabricante). - Debe Proporcionar la capacidad para marcar, tanto manual como automáticamente, determinada actividad como falso positivo, evitando además que ocurran detecciones similares. - Debe Proporcionar un análisis de todo el historial de eventos. - Debe realizar la validación continua de la clasificación de amenazas. FUNCIONALIDADES DE PROTECCION CONTRA RANSOMWARE La solución de EDR debe contar con políticas predefinidas y exclusivas para la prevención de secuestro de información por ataques de ransomware, por lo cual debe incluir más de 30 estrategias de protección diferentes. Dichas estrategias deben incluir como mínimo: - Debug de Procesos. - Código dinámico. - Formato de archivo ejecutable incorrecto - Una pila con código ejecutable - El programa ejecutado no tiene instalador - Programa crítico falso. - Empaquetador falso. - File Encryptor. - Proceso oculto.

	- Ejecutable inyectado. - Proceso inyectado. - Hilo inyectado. - Suma de comprobación no válida. - Ejecución no válida. - Puntero no válido. - Inyección de kernel. - Empaquetador conocido. - Archivo malicioso detectado. - Proceso malicioso. - Ejecutable modificado. - Stack Parcialmente asignado. - Exploit de escalamiento de privilegios. - Proceso vacío. - Manipulación de pilas. - Aplicación sospechosa. - Empaquetador sospechoso. - Ejecutable manipulado. - Ejecutable no confirmado. - Ejecutable sin asignar. - Código grabable. - Prevencion automatizada en tiempo real encripcion de Ransomware. FUNCIONALIDADES DE REMEDIACION La Solución de EDR propuesta debe orquestar operaciones de respuesta a incidentes utilizando playbooks predefinidos en la solución, optimizando sí la respuesta a incidentes y los procesos de remediación, revirtiendo de modo automático los cambios maliciosos realizados por amenazas ya contenidas, en un único dispositivo o en dispositivos distribuidos a lo largo del entorno de la entidad, las características de remediación deben cumplir como mínimo con los siguientes requerimientos: - Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta. - Debe estandarizar los procedimientos de respuesta a incidentes con la automatización de playbooks - Debe optimizar los recursos de seguridad, automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la finalización de procesos maliciosos, la reversión de cambios persistentes, la notificación a los usuarios, el aislamiento de aplicaciones y dispositivos, y la apertura de tickets. - Debe permitir la respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los

	sujetos de los ataques (como por ejemplo, grupos de estaciones de trabajo). - Debe proporcionar visibilidad completa de la cadena de ataque y los cambios maliciosos, mediante el seguimiento de código. - Debe permitir automatizar la limpieza y reversión de los cambios maliciosos preservando así la integridad del sistema. - La solución de EDR Se debe contar un servicio de respuesta y detección gestionada (MDR) ante incidentes, proporcionado por técnicos del propio fabricante - Debe realizar la contencion y respuesta de forma automatica - Debe automatizar la clasificación de incidentes y mejora la relación señal/alerta. FUNCIONALIDADES DE INVESTIGACION La solución de EDR debe enriquecer automáticamente los registros de los eventos con información detallada sobre el malware antes y después de la infección, para realizar análisis forenses en los endpoints infiltrados. Su interfaz guiada debe proporcionar una guía útil, mejores prácticas y sugerir los próximos pasos lógicos a los analistas de seguridad, estas características de investigación deben cumplir como mínimo con los siguientes requerimientos: - Debe desactivar y bloquear automáticamente las amenazas, lo que permite a los analistas de seguridad cazar marcando sus propios tiempos. - Debe contar con una tecnología propietaria de rastreo de código, permitiendo así visualizar la cadena de ataque completa y el "paciente cero", incluso si el dispositivo está fuera de línea. - Debe conservar instantáneas de memoria, de los ataques sin archivo o file-less para la búsqueda de amenazas basada en memoria. - La interfaz grafica debe mostrar explicaciones claras por qué el evento está marcado como sospechoso o malicioso, enumera el marco de ataque MITRE correspondiente, así como el siguiente paso lógico para la investigación forense. FUNCIONALIDADES DE EDR La solución de EDR debe tener la capacidad de poder integrarse con diferentes plataformas de seguridad, creando así un marco robusto que pueda identificar y responder eficiente y eficazmente frente a los ataques como es recomendado por Gartner. La solución de EDR debe poder integrarse con las siguientes plataformas: - Next Generation Firewall de la Entidad

	- Control de Acceso a la Red. - SandBoxing. - Deception o Honeypots - Correlacionador de Eventos, SIEM. - Plataforma de Orquestacion, automatización y respuesta a incidentes, SOAR. - Plataforma de Análisis de comportamiento de usuario UEBA - Plataforma de Manejo de Identidades, IAM - Debe contar con una Gestion Unificada. - Debe contar con la funcionalidad de IDENTIFICACIÓN DE INCIDENTES ENTRE PRODUCTOS - Debe contar con la funcionalidad de INVESTIGACIÓN IMPULSADA POR INTELIGENCIA ARTIFICIAL - Debe contar con la funcionalidad de RESPUESTA AUTOMATIZADA **COMPONENTES DE LA SOLUCION DE EDR** La plataforma de seguridad del endpoint EDR debe ser una arquitectura distribuida, la cual debe constar de una agente en software el cual debe ser compatible con los siguientes sistemas operativos y entornos, en versiones de 32 y 64 bits: - Windows: XP SP2/SP3, 7, 8, 8.1 y 10. - Windows Server: 2003 R2 SP2, 2008 R2 SP2, 2012, 2012 R2, 2016 y 2019. - MacOS: Yosemithe (10.10), El Captain (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15). - Linux: Redhat Enterprise Linux and CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 and 7.7, y Ubuntu LTS 16.04.5, 16.04.6, 18.04.2 server, en 64-bit. - Entornos VDI: VMWare Horizons 6 y 7, y Citrix Desktop 7. - En cuanto al hardware, se debe ser un agente muy ligero; el cual no debe requerir más de 100MB de memoria RAM, y 20MB de espacio en disco. - Adicional la solución debe permitir ser desplegada de cualquiera de las siguientes maneras: - Nube: En la Nube del Fabricante. - On-Premise: En el Datacenter de la entidad. - Hibrida: En Nube y On-premise. - AirGapped o Sistemas Cerrados.
2 Switches FORTISWITCH 548D	Renovación 5 años Seriales (S548DF5019000768,S548DF5019000791)

11 FORTIAP 221E	Renovación 5 años Seriales (FP221ETF18009680, FP221ETF18037042, FP221ETF18038400, FP221ETF18059446, FP221ETF18066616, FP221ETF18067032, FP221ETF18067185, FP221ETF18067189, FP221ETF18067240, FP221ETF18067241, FP221ETF19004515)

CLÁUSULA SEGUNDA. OBLIGACIONES DE EL CONTRATISTA: Debido al presente contrato, EL CONTRATISTA se obliga a: Cumplir con el objeto del contrato en la forma y dentro del plazo establecido en el contrato, de conformidad con las especificaciones técnicas señaladas en los estudios previos, en los pliegos de condiciones y en la propuesta.1) Presentar al momento de entregar los equipos el certificado por parte del fabricante de que los mismos están completamente configurados de fábrica y que no son remanufacturados, dado que no se admiten upgrades locales. Y las certificaciones de garantía por parte del fabricante donde conste que la garantía es en sitio y por el tiempo establecido. 2) Realizar las entregas oportunamente en la Lotería de Medellín. Los costos de movilización de los elementos al sitio de entrega indicado por el supervisor serán a cargo del contratista. 3) Entregar a la Lotería de Medellín, los bienes objeto del contrato con el cumplimiento de las especificaciones mínimas y calidad exigida en el pliego de condiciones y fichas técnicas. En caso de no cumplir estas condiciones a satisfacción de la Lotería de Medellín, el contratista se obliga a remplazarlos sin costo alguno, con relación a los elementos cuya falla o defecto sea imputable a la mala calidad, en el plazo indicado por la institución. 4) Adjuntar el certificado de garantía emitido por el fabricante con las especificaciones descritas en el pliego. 5) Atender las recomendaciones que realice la Lotería de Medellín por intermedio del supervisor del contrato. 6) Realizar migración del sistema de seguridad actual de la lotería de Medellín, garantizando que la configuración se implemente en los nuevos equipos objeto del contrato. 7) Coordinar con la persona encargada del almacén de la Lotería de Medellín la entrega de los elementos solicitados en ejecución del contrato. 8) Reemplazar los productos defectuosos o que no cumplan con las especificaciones técnicas exigidas por la Entidad, dentro de los ocho días hábiles siguientes a la fecha de notificación. 9) Presentar al supervisor del contrato informes técnicos en caso de requerirlos. 10) Cumplir con la obligación de la afiliación y pago de los aportes al sistema de seguridad social integral y ARP de sus empleados. 11) Presentar de manera oportuna la factura correspondiente al contrato y los soportes de producción y/o entrega de los productos, previo cumplimiento de los trámites administrativos, fiscales vigentes y requisitos de Ley. 12) Informar oportunamente al Contratante cuando exista o sobrevenga alguna de las inhabilidades e incompatibilidades previstas en la constitución y la ley. 13) Toda la Solución debe ser de la misma marca, ya que se busca homologación y administración centralizada. 14) La solución debe incluir todo lo necesario para que funcione correctamente; cables, software, tranceivers, tomas de conexión a energía, FC y sus respectivos conectores en ambos extremos, y todo lo necesario para el correcto funcionamiento de la misma. 15) El proveedor debe entregar la solución completamente operativa. 16) Garantía de cinco (5) años en todas las partes 7x24 – Mano de obra y en sitio (NBD) directo del fabricante. La garantía debe ser por escrito y certificada por el fabricante en todas las partes y en la totalidad de la configuración entregada. Se debe entregar el certificado de garantía. 17) Tiempos de respuesta: Los cambios de partes o de la totalidad del equipo no pueden sobrepasar los 2 días calendario. Mientras dure el trámite de garantía el contratista se compromete a instalar un equipo o dispositivo provisional, mínimo de las mismas características del retirado y en las próximas 24 horas hábiles. 18) Para cada ítem o tecnología a implementar del proyecto, el proveedor debe acreditar de sus implementadores; acta de grado o copia del diploma, el título de ingeniero adicionalmente debe presentar las certificaciones del fabricante como implementador de esta tecnología. 19) El proveedor debe certificar su

experiencia en este tipo de proyectos, atreves de carta de recomendación de tres clientes. 20) Los equipos deben venir completamente configurados de fábrica, no se admiten upgrades locales para cumplir con los requisitos del pliego y esto debe estar certificado por el fabricante al momento de presentar la oferta y a la entrega de los equipos. 21) Todo el hardware debe contar con herramientas de software propietaria del fabricante que permita hacer gestión del equipo y del sistema operativo. 22) Se deben incluir 20 horas de capacitación sobre la solución implementada en las instalaciones de la Lotería de Medellín. 23) Las propuestas deben especificar las referencias, modelos y caracteristicas de los equipos propuestos. Incluir ficha técnica del fabricante. 24) El proveedor debe entregar la documentación de la implementación, los pasó a paso de como quedo implementada la solución y las aplicaciones contratadas. 25) Pagar los impuestos, tasas y contribuciones a que haya lugar. CLÁUSULA TERCERA. OBLIGACIONES DE LA CONTRATANTE: LA CONTRATANTE se obliga para con EL CONTRATISTA a: 1) Realizar el pago del contrato según la forma establecida en el contrato. 2) Poner a disposición del Contratista la información necesaria para el desarrollo de las actividades que se requiera ejecutar. 3) Informar cualquier novedad o modificación a la planeación con mínimo 10 días hábiles de la ejecución de las actividades programadas. 4) Los permisos necesarios de Ingreso del personal requerido durante el tiempo de la Implementación. 5) Disponibilidad para pruebas del producto entregado. CLÁUSULA CUARTA. PLAZO DE EJECUCIÓN: El plazo de ejecución del contrato será de cuatro (4) meses contados desde la suscripción del Acta de Inicio. CLÁUSULA QUINTA. VALOR DEL CONTRATO Y FORMA DE PAGO: VALOR: El valor total del contrato será de hasta DOS MIL TRECIENTOS CINCUENTA MILLONES DOSCIENTOS NOVENTA Y OCHO MIL CIENTO NOVENTA PESOS M.L.C. ($2.350.298.190) IVA incluido. FORMA DE PAGO: Los valores causados a favor del contratista con ocasión de la ejecución del presente contrato, le serán cancelados previa presentación de las respectivas facturas o cuentas de cobro en original y dos (2) copias, acompañadas de los respectivos informes de las actividades desarrolladas durante el periodo facturado; las cuales en todos los casos deben contar con el visto bueno del supervisor del contrato en señal de que el bien y/o servicio contratado ha sido recibido a plena satisfacción de la entidad. Se debe tener en cuenta que en caso de que uno de los ítems solicitados no se compre por solicitud de Lotería de Medellín, este deberá ser descontado del valor del contrato. CLÁUSULA SEXTA. APROPIACIÓN PRESUPUESTAL: Para la suscripción del presente contrato, LA CONTRATANTE ha constituido la Disponibilidad presupuestal N° 617 del 02 de septiembre de 2024 con cargo a los siguientes rubros: 1.1.08.10.2.3.2.01.01.003.03.032 GV_DI_TI_Maquinaria y equipo_(1.7_PROYECTOS DE RENOVACIÓN TECNOLÓGICA) y 1.1.08.10.2.3.2.01.01.005.02.033 GV_DI_TI_Otros activos fijos_(1.7_PROYECTOS DE RENOVACIÓN TECNOLÓGICA), de la actual vigencia por valor de DOS MIL TRESCIENTOS SETENTA MILLONES CINCUENTA Y CUATRO MIL TRECIENTOS SETENTA Y SIETE PESOS ($2.370.054.377) y compromiso presupuestal 1397 del 11 de octubre de 2024, por valor de DOS MIL TRECIENTOS CINCUENTA MILLONES DOSCIENTOS NOVENTA Y OCHO MIL CIENTO NOVENTA PESOS M.L.C. ($2.350.298.190). CLÁUSULA SÉPTIMA. CONFIDENCIALIDAD: EL CONTRATISTA se obliga a guardar confidencialidad en relación con cualquier información, datos o documentos que hayan sido recibidos de LA CONTRATANTE en el curso de la negociación, celebración y ejecución del presente contrato. EL CONTRATISTA no podrá utilizar dicha información, datos o documentos confidenciales para fines distintos a los requeridos para la ejecución del presente contrato, ni podrá publicar o divulgar a terceros dicha información, datos o documentos salvo en los siguientes casos: a) Cuando así lo exijan las disposiciones legales vigentes. b) Cuando así lo exija una autoridad competente. c) Con autorización previa por escrito de LA CONTRATANTE. CLÁUSULA OCTAVA. CLÁUSULA PENAL PECUNIARIA: LA CONTRATANTE podrá imponer a EL CONTRATISTA, en caso de declaratoria de incumplimiento o retardo en el cumplimiento del objeto contractual dentro del

plazo establecido para el efecto, como pena, una suma equivalente al diez por ciento (10%) del valor del contrato. El valor de la cláusula penal que se haga efectiva se considerará como pago parcial de los perjuicios causados a LA CONTRATANTE, sin perjuicio que de que ésta pueda cobrar los perjuicios probados y exigir el cumplimiento del objeto contractual. La Entidad podrá descontar el valor de la cláusula penal directamente de los saldos que se adeuden al contratista, o de la garantía constituida, y si no fuere posible hará efectivo su cobro por vía judicial, para lo cual el presente contrato prestará mérito ejecutivo y EL CONTRATISTA manifiesta que renuncia a cualquier requerimiento judicial o prejudicial. CLÁUSULA NOVENA. GARANTÍAS: Una vez suscrito el presente contrato, constituirá, a favor de la LOTERÍA DE MEDELLÍN como mecanismo de cobertura del riesgo derivado del incumplimiento de las obligaciones legales o contractuales, cualquiera de las garantías autorizadas por el Decreto 1082 de 2015, a saber: (1) Contrato de seguro contenido en una póliza, (2) Patrimonio autónomo, (3) Garantía bancaria, con el fin de cubrir los incumplimientos derivados de las obligaciones contractuales amparando los siguientes riesgos: De Cumplimiento: Su valor no será inferior al 10% del valor del contrato y su vigencia será por el término del contrato y seis (6) meses más. De Calidad del servicio: Su valor no será inferior al 10% del valor del contrato y su vigencia será por el término del contrato y seis (6) meses más. CLÁUSULA DÉCIMA. CAUSALES DE TERMINACIÓN: El presente Contrato se podrá dar por terminado por las siguientes causas: A) Cuando se alcance y se cumpla totalmente el objeto del contrato. B) Por mutuo acuerdo de las partes, siempre que la terminación no implique renuncia a derechos causados o adquiridos a favor de las partes. C) Cuando por razones de fuerza mayor o caso fortuito de conformidad con la Legislación Colombiana se haga imposible el cumplimiento de los objetivos propuestos. D) Por el incumplimiento de cualquiera de las obligaciones establecidas para cada una de las Partes. E) Por vencimiento del término fijado para la ejecución del mismo. F) Por las demás causales señaladas en la ley. PARÁGRAFO. Efectos de la Terminación: Una vez terminado el Contrato, en caso de ser requerido, las partes suscribirán la correspondiente acta de liquidación, señalando los compromisos que deban subsistir aun cuando obre la liquidación a fin de terminar las actividades que se encuentran en curso. CLÁUSULA DÉCIMA PRIMERA. INDEMNIDAD: EL CONTRATISTA, mantendrá indemne y libre de daño y defenderá a LA CONTRATANTE y cada uno de los respectivos funcionarios, directores, empleados, representantes y contra todo reclamo, requerimiento, demandas, juicio, procedimiento, mandatos judiciales, sentencias, órdenes y decretos presentados, realizados o pronunciados en contra de todos o de cualquiera de ellos y todos los daños, pérdidas y expensas sufridas o incurridas por ellos o por cualquiera de ellos resultantes y que sean imputables a EL CONTRATISTA. CLÁUSULA DÉCIMA SEGUNDA. CESIÓN DEL CONTRATO: El presente contrato no podrá ser cedido parcial o totalmente a ninguna persona natural o jurídica, pues se entiende celebrado en consideración a la persona de EL CONTRATISTA. CLÁUSULA DÉCIMA TERCERA. PERFECCIONAMIENTO, LEGALIZACIÓN Y EJECUCIÓN: El presente contrato se perfeccionará con la firma del mismo y su ejecución iniciará una vez se aprueben las pólizas, si se requirieron, se expida el Compromiso Presupuestal y posteriormente las partes firmen el Acta de Inicio. CLÁUSULA DÉCIMA CUARTA. EXCLUSIÓN DE RELACIÓN LABORAL: LA CONTRATANTE NO ADQUIERE ningún vínculo de carácter laboral con EL CONTRATISTA, sus empleados, agentes, administradores y cualquier persona que esté bajo su dependencia o subordinación. EL CONTRATISTA es el único responsable del pago de las prestaciones y demás derechos laborales adquiridos por el personal que se encuentre a su cargo. CLÁUSULA DÉCIMA QUINTA. SUPERVISIÓN: LA CONTRATANTE designará como supervisor del contrato al Jefe de la Oficina TIC de Lotería, o a quien haga sus veces. PARÁGRAFO PRIMERO: LA CONTRATANTE, podrá modificar el supervisor del contrato

cuando lo considere necesario, sin que esto implique una modificación al contrato que se suscribe. PARÁGRAFO SEGUNDO: Se deberá anexar para cada pago el informe de supervisión del contrato, el cual debe ser realizado en el formato establecido por la Entidad para tal efecto. CLÁUSULA DÉCIMA SEXTA. INHABILIDADES E INCOMPATIBILIDADES: EL CONTRATISTA, declara que para la celebración de este contrato no se encuentra incurso dentro de las inhabilidades e incompatibilidades consagradas en la Ley; como señal de ello, diligencia y firma el formato de inhabilidades, impedimentos, incompatibilidades y conflictos de intereses establecido en la entidad. CLÁUSULA DÉCIMA SÉPTIMA. CUMPLIMIENTO OBLIGACIONES PARAFISCALES Y DEL SISTEMA DE SEGURIDAD SOCIAL INTEGRAL: Es una obligación de EL CONTRATISTA el cumplimiento de sus obligaciones frente al Sistema de Seguridad Social Integral, Parafiscales (Cajas de Compensación Familiar, Sena e ICBF) cuando a ello haya lugar, por lo cual el incumplimiento de esta obligación será sancionado de acuerdo a la normatividad vigente para el caso particular. CLÁUSULA DÉCIMA OCTAVA. OBLIGACIÓN ESPECIAL SOBRE PREVENCIÓN DEL LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO. LAS PARTES se obligan a no utilizar el objeto de este contrato, como instrumento para el ocultamiento, manejo, inversión o aprovechamiento, en cualquier forma de dinero u otros bienes provenientes de actividades delictivas, o para dar apariencia de legalidad a actividades delictivas, a transacciones o a fondos vinculados con las mismas y a informar, inmediatamente, cualquier sospecha o información que llegare a conocer relacionada con este tema, respecto de las obligaciones derivadas del presente contrato. PARÁGRAFO. El CONTRATISTA autoriza a la LOTERIA DE MEDELLÍN a ejercer todas las acciones correspondientes para dar cumplimiento al Acuerdo 574 de 2021, por medio del cual se establecen los requisitos para la adopción del Sistema de Administración de Riesgos de Lavado de Activos, Financiación del Terrorismo y la Proliferación de Armas de Destrucción Masiva, SARLAFT, y demás normas que lo modifiquen, adicionen o sustituyan. CLÁUSULA DÉCIMA NOVENA. TRATAMIENTO DE DATOS PERSONALES. Las PARTES manifiestan su autorización expresa y recíproca para que las informaciones de carácter personal de sus dependientes y colaboradores que tenga participación e incidencia directa en la ejecución del presente contrato, sea almacenada en las bases de datos de cada una de las PARTES y sometida a tratamiento para los fines del presente negocio jurídico, con estricta observancia de las disposiciones contenidas en la Ley 1581 de 2012, y demás normas reglamentarias. Así las cosas, dicha información podrá ser almacenada, consultada, administrada, verificada y/o actualizada, con la finalidad de llevar a cabo actuaciones propias del objeto social de las PARTES contratantes y, en general, cualquier acto propio del giro ordinario de sus negocios, de conformidad con las políticas de tratamiento de datos e informaciones de carácter personal adoptadas por cada una de ellas, según el caso, las cuales han sido puestas a disposición de manera recíproca para consulta. CLÁUSULA VIGÉSIMA. SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES: En caso de que surjan diferencias entre las partes por razón o con ocasión del presente Contrato, podrán ser resueltas por ellas de buena fe y mediante arreglo directo; para tal efecto, las partes dispondrán de diez (10) días calendario, contados a partir de la fecha en que cualquiera de ellas requiera a la otra, por escrito en tal sentido, término éste que podrá ser prorrogado de común acuerdo. Adicionalmente las partes acuerdan que para la solución de las diferencias y discrepancias que surjan de la celebración, ejecución, terminación o liquidación de este contrato, podrán acudir a los procedimientos de transacción o conciliación establecidos por la Ley. CLÁUSULA VIGÉSIMA PRIMERA. LIQUIDACIÓN: La liquidación del Contrato se hará de común acuerdo entre EL CONTRATISTA y LA CONTRATANTE, dentro de los cuatro (4) meses siguientes a la fecha de su terminación. Dentro de este plazo y sin que ninguna de las partes haya solicitado una extensión o prórroga al término dispuesto, las

partes acordarán los ajustes, revisiones y reconocimientos a que haya lugar, de los cuales quedará constancia en el acta de liquidación. De solicitarse la extensión o prórroga para finiquitar la liquidación no podrá ser mayor a ciento veinte (120) días adicionales. Si EL CONTRATISTA no concurre a la liquidación del Contrato, o las partes no llegan a un acuerdo sobre su contenido, LA CONTRATANTE lo liquidará unilateralmente dentro de los dos (2) meses siguientes al vencimiento de los cuatro (4) meses previstos o de su prórroga para la liquidación bilateral, quedando EL CONTRATISTA con el derecho de recurrir legalmente por vía de conciliación o por la vía judicial correspondiente para todo aquello en que no haya concurrido con LA CONTRATANTE. CLÁUSULA VIGÉSIMA SEGUNDA. DOMICILIO Y NOTIFICACIONES: Para todos los efectos se acuerda como domicilio la ciudad de Medellín, Departamento de Antioquia, República de Colombia, las notificaciones y comunicaciones a las siguientes direcciones: LA CONTRATANTE: Carrera 47 No. 49-12, Medellín. EL CONTRATISTA: Carrera 48 No. 48C sur 86, oficina 2213, Correo Electrónico: contactenos@jitsolutions.com.co

Para constancia se firma en Medellín, el 18 OCT. 2024

OCTAVIO DE JESÚS DUQUE JIMÉNEZ
LOTERÍA DE MEDELLÍN

CAMILO ANDRÉS BAHAMÓN GENE
EL CONTRATISTA

	NOMBRE	CARGO	FIRMA
Proyectó	Edwar Andrés Orozco Giraldo	Asesor Jurídico	
Revisó	Isabel Posada Barrera	Secretaria General	
Los firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y por lo tanto bajo nuestra responsabilidad lo presentamos para firma.			