FORMATO 7

ANEXO TECNICO

El suscrito proponente del Proceso de Selección Invitación Pública de Mínima Cuantía No.MC-021-2024 me comprometo por medio del presente documento a cumplir con las especificaciones técnicas del objeto a contratar y que se describen a continuación:

Servicio de licenciamiento de antivirus FortiClient y puesta en marcha en todos los equipos de cómputo de la entidad.

Item	Cantidad	Descripción	
1	100	Licencia	FortiClient 1 año: Endpoint-based Licenses - EPP/ATP FortiClient EPP/ATP Includes VPN/ZTNA Agent, EPP/ATP and EMS hosted by FortiCloud with FortiCare Premium SSL inspection, Inline AV and anti-malware, intrusion prevention (IPS), FortiGuard web and video filtering, DNS security, USB device control. Zero Trust Agent with Multi-factor Authentication (MFA), Central Management via EMS or FortiClient Cloud, Central Logging and Reporting, Dynamic Security Fabric Connector, Vulnerability Agent and Remediation, SSL VPN with MFA, IPsec VPN with MFA, FortiGuard Web Filtering, Split-tunneling, Single Sign-on (SSO). AI-powered Next-Generation Antivirus (NGAV), FortiClient Cloud Sandbox, Automated Endpoint Quarantine, Application Firewall, Application Inventory. La solución deberá ser 100% compatible con la plataforma de NGFW con la que ya cuenta la entidad (FortiGate 100F) y deberá

				integrarse de forma nativa con la misma, para lo cual no requerirá de desarrollo adicional alguno. Debe ser compatible con los siguientes sistemas operativos: Microsoft Windows: 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits) e 10 (32 e 64 bits); Microsoft Windows Server: 2008 R2 o superior; Mac OS X: v10.8, v10.9, v10.10, v10.11; Linux: Ubuntu 16.04 o superior, Red Hat 7.4 o superior, CentOS 7.4 o superior. Permitir la copia de seguridad del archivo de configuración del endpoint. Generar bitácora (logs) sobre las funcionalidades instaladas y configuradas. Enviar los registros (logs) a la consola de gestión central. Funcionalidades de Antivirus El cliente de seguridad debe ser capaz de inspeccionar archivos ejecutables, librerías y drivers en busca de virus, de enviar archivos para ser inspeccionados en sistemas de Sandboxing del mismo fabricante, notificar localmente cuando se detecta un virus, permitir que el usuario comience un escaneo bajo demanda, permitir que se comience escaneo de virus de forma automática regularmente, permitir visualizar los archivos puestos en cuarentena, permitir la configuración del perfil antivirus desde la consola central del mismo fabricante. Funcionalidades de Filtrado de Contenido Web

			Debe permitir la configuración del perfil de filtro de web desde la consola central del mismo fabricane, disponibilizar consultas en línea desde el cliente de seguridad sobre la categoría de determinada web (por ej. Interés general, tecnología, hacking, pornografía, etc) para aplicar política de control de acceso a internet, admitir reglas estáticas de acceso a internet basado en expresiones regulares. Funcionalidades de Firewall de Aplicación Debe admitir perfiles de Control de Aplicaciones creados centralmente desde la consola de gestión del mismo fabricante, reconocer más de 2800 aplicaciones por el cliente para ser usadas en reglas de control de acceso. Funcionalidades de Scanner de Vulnerabilidades Debe tener integrado un módulo de búsqueda de vulnerabilidades y permitir la gestión central desde la consola del mismo fabricante, permitir que el usuario comience un análisis de vulnerabilidades bajo demanda, las vulnerabilidades encontradas deben ser mostradas localmente con un vínculo para visualizar información desde una base de datos en internet, debe tener al menos: nombre, severidad y detalles.
		Implementación	Implementación de políticas y perfiles de seguridad en el antivirus de acuerdo con las necesidades de la entidad. configuración, soporte y puesta en marcha.
2	1	Instalación, implementación, integración, configuración, puesta en marcha y soporte de la plataforma de	

		administración (consola), y la instalación del antivirus en todos los 100 equipos de la entidad, de forma presencial, con el personal idóneo y capacitado.
3	1	Soporte remoto para la infraestructura tecnológica de la alcaldía (Red, Firewall, Antivirus, demás), corresponde a una bolsa de 8 horas a demanda y necesidad.
4	1	Certificación de distribuidor o mayorista autorizado directamente del fabricante, anexar certificación, dirigida a la entidad.

Respetuosamente,

Nombre o Razón Social del Oferente: ROYAL TECH GROUP SAS
N.I.T. 9013946552
Nombre del Representante Legal: HÉCTOR DAVID MENDOZA ARROYO
C.C. No. 1140834004 de Barranquilla
Dirección: CRA 22C NO 68 - 65
Teléfono: 3155482662
Fax: 3155482662
Firma: _____

HECTOR MENDOZA ARROYO