DETALLE DE LAS ESPECIFICACIONES TÉCNICAS PARA ADQUISICIÓN DE BIENES	**Código:** SNMLCF-CGAF-FOR-001-2022	
	Versión: 1.0	**Fecha:** 11/07/2022
	Página **1** de **11**	

DATOS GENERALES	
NÚMERO:	SNMLCF-DTIC-2024-087
ENTIDAD CONTRATANTE:	SERVICIO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES
OBJETO DE LA CONTRATACIÓN	ARRENDAMIENTO DEL SERVICIO, INCLUIDO ACTUALIZACIÓN Y SOPORTE PARA LA PLATAFORMA DE ANTIVIRUS DEL SERVICIO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES.
CPC A NIVEL 5	73310
DESCRIPCIÓN DEL CPC	CONCESION DE LICENCIAS PARA EL DERECHO DE USO DE PROGRAMAS DE COMPUTACION
CPC A NIVEL 9	733100011
DESCRIPCIÓN DEL CPC	SERVICIOS PARA PERMITIR, OTORGAR O AUTORIZAR DE OTRA MANERA EL USO DE DERECHOS PARA UTILIZAR PROGRAMAS DE COMPUTACION, DESCRIPCION DE PROGRAMAS Y MATERIALES DE APOYO PARA SISTEMAS Y APLICACIONES DE SOFTWARE
UNIDAD REQUIERENTE:	Dirección de Tecnologías de la Información y la Comunicación
FECHA:	13 de agosto de 2024

No.	**TIPO DE SERVICIO**	**DESCRIPCIÓN DEL SERVICIO**		**LUGAR DE ENTREGA**
1	ARRENDAMIENTO DEL LICENCIAMIENTO, ACTUALIZACIÓN Y SOPORTE DE LA PLATAFORMA DE PROTECCIÓN ANTIVIRUS DEL SNMLCF	**TIPO DE SERVICI**	"ARRENDAMIENTO DEL LICENCIAMIENTO, ACTUALIZACIÓN Y SOPORTE DE LA PLATAFORMA DE PROTECCIÓN ANTIVIRUS DEL SNMLCF"	SNMLCF-Quito Edificio Matriz (Av. Mariana de Jesús y Av. Occidental. sector La Granja, cantón Quito)
		ESPECIFICACIONE TÉCNICAS	**DETALLE**	
		CANTIDAD	750 licencias Al menos 15 de estos equipos deben contar con licencias que incluyan tecnologías XDR y funcionalidades avanzadas de protección proactiva y caza de amenazas.	
		Defensa básica	Antimalware Mejorado	
			Gestión de vulnerabilidades	
			Supervisión de procesos	
			Supervisar el sistema UEFI.	
			Firewall.	
			Gestion de firewall a nivel local	

				Protección asistida en la nube atreves de la red de Seguridad		
				Analizar los sectores de arranque en búsqueda de amenazas persistentes.		
				Agente integrado de detección y respuesta para endpoints		
				Incluir un agente independiente que actúe incluso cuando no hay conexión.		
				Control de Aplicaciones basado en listas negras		
				Control Web		
				Seguridad para trafico de red en protocolos HTTPS, RDP, FTPS, SCP y SSH		
				Control de Dispositivos		
				Monitorización de recursos compartidos		
				Protección de servidores		
				Investigación de incidentes		
				Protección para servidores		
				Reglas de asignación de politicas		
				Malware Sandbox manual y automático		
				Análisis de tráfico cifrado HTTPS, FTPS, SSH		
				Configuración e implementación del sistema		
				Acceso a la consola por comunicación cifrada https		
				Exploits de software ante vulnerabilidades conocidas y desconocidas		
				Prevención de ransomware		
				Mitigación de ransomware		
				Anti-Malware para virus, troyanos, spyware, adware.		
				Amenazas avanzadas		
				Amenazas sin archivos		
				Ataques de powerShell		

	Ataques dirigidos y técnicas ATT&CK
Firewall personal	Firewall debe permitir crear reglas para filtrado de aplicaciones.
	Firewall debe permitir crear reglas para filtrado de conexiones.
	Firewall debe permitir configurar las diferentes redes como: local, público o de confianza.
	El firewall local debe detectar y bloquear conexiones relacionadas a descubrimiento de puertos.
	Debe tener un módulo de protección contra ataques de red.
	Debe permitir crear excepciones en el módulo de protección contra ataques de red.
Administración	La consola de administración deberá permitir administrar de forma remota, ejecutando las versiones antivirus en clientes finales y servidores de las diferentes plataformas (Windows, Linux, Mac OS)
	Dashboard con información de estado del producto en los clientes.
	Integración con directorio activo.
	Capacidad de gestionar y controlar subconsolas bajo su jurisdicción que poseen sus propios licenciamientos
	Consola multi-tenant y con capacidad de crear varios grupos de administración.
	Manejo de grupos jerárquicos de endpoints.
	Administración Basada en roles.
	Capacidad de Administrar servidores y clientes Linux y clientes Mac a través de la consola de administración.
	Administración centralizada del antivirus mediante políticas.
	La consola de administración deberá permitir actualizar a través del servidor de la solución a todas las estaciones protegidas

				Las actualizaciones de las bases de datos de firmas de códigos maliciosos del producto antivirus deberán ser incrementales, evitando de esta manera el ancho de banda en su despliegue.		
				Calendarización de tareas tanto de análisis como de actualización.		
				Permitir detener o activar escaneo de virus PCs individuales, desde la consola.		
				Capacidad de recibir notificaciones sobre nuevas versiones de las aplicaciones corporativas del producto.		
				Permitir sincronización de la estructura de Active Directory con la de los grupos de administración.		
				Permitir la configuracion de los agentes/servidores de actualización locales.		
				Permitir soporte de Virtual Desktop Infrastructure (VDI).		
				Consola de alta disponibilidad de conexión.		
				Bloqueo del endpoint con contraseña para evitar cambios no autorizados.		
				Permite envío automático de reportes a usuarios específicos de correo.		
				Reportes exportables mínimo a CSV y PDF.		
				Debe permitir la personalización de intervalo de tiempos de datos sobre los reportes.		
				Multidifusión de politicas de configuracion.		
				Debe poder cambiar o robustecer la configuración de los endpoints al detectar un brote de virus en la red desde la consola general de administracion.		
				Análisis de conexiones por RDP o SSH.		
				Debe tener una arquitectura basada en la nube como servicio.		
				Notificaciones de grupos de estaciones a usuarios específicos de correo.		
				Capacidad para administrar más de 1.000 dispositivos sobre una misma consola.		

				Capacidad de visualizar de manera consolidada los dispositivos gestionados, sus características técnicas, como sistema operativo y versión, Nombre de dispositivo y dirección IP, Tipo de infección		
				Capacidad de buscar eventos de seguridad pasados con el uso de criterios de búsqueda complejos de parámetros ya sean de red, proceso, archivo, registros, recursos y más.		
				La consola de administración debe permitir manejar múltiples políticas de seguridad, pudiendo activar una política específica ante epidemias de virus		
				Permitir crear políticas especiales con distintas seguridades y asignarlas a grupos determinados de equipos		
				Controlar a través de políticas todos los componentes mencionados previamente (para estaciones de trabajo y servidores), sin necesidad de consolas adicionales de administración		
				Delegación de tareas mediante la creación de usuarios con distintos perfiles de administración		
				Permitir reversar configuraciones o ajustes de politicas.		
				Comunicación Cifrada o SSL entre la consola y los clientes, a través de certificados digitales propios o de terceros		
				Distribución de agentes, configuraciones y actualizaciones de forma centralizada		
				Facilidad para accesar a la consola desde cualquier sitio en la red		
				Monitoreo permanente y generación reportes de eventos en tiempo real		
				Permite desde sitio central la distribución masiva del agente		
				Facilidad en la actualización del agente para usuarios fuera de la red		
				Establecer políticas por grupos de trabajo y estructuras de herencia		

	Desactivar y desinstalar el agente de manera segura y remota.
	Consola Web
	Alojamiento de la información de detecciones por al menos 90 días.
	Windows 10
Compatibilidad con Sistemas Operativos Windows 32 y 64 bits	Windows 8
	Windows 7 SP1
	Windows 10
	Windows 11
	Windows 2008 R2
	Windows 2012
	Windows 2016
Compatibilidad con Sistemas Operativos Linux 32 y 64 bits	AlmaLinux 8.x en adelante
	Red Hat Enterprise Linux 7.X Desktop; en adelante
	Red Hat Enterprise Linux 8.X Desktop; en adelante
	Fedora 36 a 39;
	CentOS 7.X; en adelante
	SUSE Linux Enterprise Desktop 12 SP4 y SP5
	SUSE Linux Enterprise Desktop 15 SP1 – SP5;
	OpenSUSE Leap 15.2 -15.4;
	OpenSUSE Leap 15.4;
	Debian GNU/Linux 9 - 12;
	Linux Mint 20.x en adelante;
	Ubuntu 16.04x; en adelante
	Debian 9 en adelante
Compatibilidad con Sistemas Operativos Mac	Mac OS 14.X (Sonoma)
	Mac OS 13.X (Ventura)
	Mac OS 12.X (Monterey)

				Mac OS X 11.X (Big Sur)	
				Debe permitir realizar una Instalación Remota	
			Otras Características	Debe permitir desinstalar otros productos antivirus al momento de realizar la instalación	
				Debe proteger los archivos de instalación a fin de evitar que se corrompan durante la instalación en un equipo infectado	
				La consola debe permitir gestionar los equipos instalados bajo políticas de proteccion y la posibilidad de enviar tareas en simultáneo o programadas.	
				Detección mínima de falsos positivos o falsos virus.	
				Mantener tecnologías de Machine Learning y heurística proactiva para las detecciones.	
				Inventario básico de software vulnerable por falta de actualizaciones dentro de los equipos.	
			Funciones adicionales	Debe poder desactivar el arranque automático de dispositivos extraíbles.	
				Monitoreo de paquetes enviados por la red.	
				Compatibilidad certificada con plataforma de virtualización VMWare y Xen.	
				Posibilidad de realizar integración con active directory y SIEM’s	
				Soportar gestión de varios administradores en la consola	
				Manejar la comunicación con los agentes, y recopilar y almacenar los datos de las aplicaciones mediante telemetria. Ser capaz de manejar decenas de miles de clientes manteniendo su elevada velocidad operativa sin saturar la infraestructura.	
				Permitir detección de incidencias a través de indicadores de compromiso en hash MD5 y SHA256	
				Permitir bloqueo de aplicaciones por lista negra de aplicaciones y por hash md5, sha256 u otros	
			Endpoint	Bloqueo para que los usuarios no puedan	

				modificar o desinstalar el agente.		
				Control de vulnerabilidades de aplicaciones que controle e identifique las vulnerabilidades de estas.		
				Control por tipo de dispositivo a ser conectado		
				Permitir a los usuarios seleccionados y / o grupos de equipos acceder a determinados tipos de dispositivos por politicas o configuraciones.		
				Permitir a los usuarios seleccionados y / o grupos de equipos ver partes determinadas el árbol de carpetas gestionado en la consola.		
				Permitir a los usuarios seleccionados y / o grupos de equipos leer el contenido de los dispositivos de almacenamiento externo.		
				Permitir a los usuarios seleccionados y / o grupos de equipos modificar el contenido de los dispositivos de almacenamiento externo.		
				Permitir la creación de dispositivos de confianza a los cuales los usuarios tienen acceso total en todo momento.		
				Control de acceso web para usuarios y / o grupos de equipos.		
				Control de acceso web mediante filtro por categoría.		
				Control de acceso para realizar permisos/bloqueos puntuales (Específicos)		
				Control de acceso a web por categorías de páginas web y horarios en simultáneo.		
				Control de acceso web filtro por direcciones URL.		
				Control de acceso web mediante reglas para determinados grupos de equipos.		
				Permitir configurar las reglas de control de acceso web mediante horario.		
				Permitir dar prioridad a cualquiera de las reglas de control de acceso web creadas.		
				Permitir configurar las reglas de control de acceso web para: permitir, bloquear o alertar el		

				acceso a los diferentes sitios.	
				Control de acceso web debe tener un analisis de protocolos http y https.	
				Debe permitir realizar un bloqueo de amenazas por hash de ejecutables en toda la red	
				Arquitectura Escalable y en Alta Disponibilidad	
			Administración de Consola y tecnologías	La solución proporciona soporte para el análisis de incidentes al proporcionar herramientas para ayudar a filtrar, investigar y tomar medidas en todos los eventos de seguridad detectados por el sensor EDR durante un intervalo de tiempo específico	
				La solución se integra con la base de conocimiento ATT & CK de MITRE y etiqueta los eventos de seguridad de manera adecuada.	
				Se debe contar con la existencia de un componente de correlación de eventos, capaz de detectar ataques avanzados en múltiples puntos finales en infraestructuras híbridas (estaciones de trabajo, servidores o contenedores, que ejecutan varios sistemas operativos).	
				En los registros de auditoría se puede dejar constancia de las acciones realizadas en la consola de administración por usuario.	
				Se deberá poder visualizar el estado de la red desde paneles portlets o widgets que sean completamente personalizables, tanto en cantidad como en contenido. Dicha información será en tiempo real y se podrá elegir si verla en formato gráfico o tabla	
				Los productos y las actualizaciones de firmas se pueden distribuir de manera más eficiente en la red gracias a un sistema que funciona a modo de transmisor.	
				Puede permitir o denegar a los usuarios la posibilidad de modificar los ajustes de seguridad para su sistema.	
				La solución ofertada deberá detectar virus en archivos compactados, con profundidad máxima (16), en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros	

	La solución deberá contar con la opción de realizar exclusiones de archivos de los análisis programados.
	Permitir prevenir las infecciones de fugas y malware datos sensibles a través de dispositivos externos conectados a extremos aplicando bloqueo normas y excepciones a través de la política a una amplia gama de tipos de dispositivos (tales como unidades Flash USB, dispositivos Bluetooth, reproductores de CD/DVD, dispositivos de almacenamiento, etc.).
	La solución puede conectarse remotamente al host mediante shell para investigar rápidamente los ataques, recopilar datos forenses y remediar las infracciones
	En la consola de administración se pueden crear cuentas internas con diferentes privilegios de acceso.
	La solución debe permitir recopilar registros básicos y avanzados de forma remota. Con el fin de facilitar el análisis en profundidad del problema y proporcionar una resolución más rápida.
	La cuarentena se almacena localmente, pero puede administrarse de manera centralizada desde la consola de control.
	Proporcionar protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común y aplicaciones propias, como el navegador, Microsoft Office o Adobe Reader, así como contra intentos específicos de post-explotación en modo kernel.
	Políticas de seguridad que se adaptan al hecho de que los usuarios utilicen sus equipos fuera de las instalaciones de la empresa.
	Brindar la posibilidad de poder realizar consultas a los incidentes mediante consultas predefinidas y personalizadas.
Funcionalidades	Brindar visibilidad de las aplicaciones vulnerables que el usuario ha instalado en los equipos

		de control de aplicaciones	Flexibilidad para aplicar políticas de control por grupos de usuarios, para bloquear aplicaciones en particular.		
			Poder manejar el inventario de aplicaciones vulnerables agrupado por el nivel de gravedad, y el estado.		
			Ofrecer la opción de marcar o ignorar aplicaciones vulnerables.		
			Poder crear listas negras para especificar qué aplicaciones se pueden ejecutar y cuáles no, por nombre de aplicación o ruta.		
			La contratista deberá realizar la actualización de las políticas actuales que posee el SNMLCF a nivel nacional y nuevas bajo las directrices y lineamientos del SNMLCF. En caso de que hubiese inconvenientes en la implementación el proveedor deberá brindar el soporte necesario para que se instale el antivirus en los equipos al 100% con apoyo de la DTIC´s del SNMLCF. Así como el funcionamiento de la solución en cada una de las sucursales, oficinas técnicas o centros forenses pertenecientes al SNMLCF.		

- Contar con al menos 08 horas de soporte técnico especializado como parte del servicio de “ARRENDAMIENTO DEL LICENCIAMIENTO, ACTUALIZACIÓN Y SOPORTE DE LA PLATAFORMA DE PROTECCIÓN ANTIVIRUS DEL SERVICIO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES”, actualización de la protección de antivirus para el SNMLCF.

INFORMACIÓN DE CONTACTO	
RESPONSABLE DEL PROCEDIMIENTO:	Francisco Rodríguez
TELÉFONO DE CONTACTO:	(02) 393-4220 Ext 406
CORREOS ELECTRÓNICOS PARA ENVÍO DE PROFORMAS:	Las proformas se podrán presentar a través del portal de Compras Públicas.

Con base en la descripción de la necesidad institucional detallada, se solicita la presentación de proformas para la provisión del servicio hasta el miércoles 14 de agosto 2024 a las 17:00 horas.

Requisitos de la proforma:

La proforma debe de forma obligatoria contender la siguiente información:

- Fecha de emisión.
- Número de proforma.
- Destinatario de la proforma **(*SERVICIO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES RUC: 1768187190001 DIRECCIÓN: AV. MARIANA DE JESÚS 21 - 30 y AV. ANTONIO JOSÉ DE SUCRE).***
- Ruc del proveedor.
- Descripción del servicio (la descripción debe corresponder a los componentes técnicos del servicio), cantidad, precio unitario y valor total.
- La empresa proveedora deberá detallar un pack del soporte especializado de 08 horas para ser aplicadas según las necesidades de la Institución sin tiempo de caducidad. Muy independientemente de los trabajos de implementación y afinamiento de los equipos y sin costo adicional para la institución.
- La empresa proveedora deberá contemplar la trasferencia de conocimientos para 4 funcionarios de la Institución por un tiempo mínimo de 4 horas, esta será sin costo adicional para la institución.
- Plazo de entrega: 20 días a partir del día siguiente a la suscripción de la orden de compra y la ejecución de la licencia será a partir de la caducidad de la misma que es el 12 de diciembre del 2024.
- Forma de pago **contra entrega**
- Vigencia de la oferta ***(al menos 90 días).***
- Datos del proveedor ***(números de contacto, dirección, correo electrónico).***
- Firma o sello del proveedor.
- **En la descripción de la proforma debe constar el CPC de la contratación tal como consta en el presente documento, a excepción de los procedimientos de ínfima cuantía.**

Documentos que debe adjuntar a la proforma:

- Copia de RUC con código QR.
- Copia de RUP con firma electrónica del proveedor.
- Fichas técnicas de los bienes con firma electrónica del proveedor.

FIRMAS DE RESPONSABILIDAD:	
Elaborado por: Firmado electrónicamente por: DIEGO FERNANDO HERNANDEZ SANCHEZ Tngl. Diego Hernández **ANALISTA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**	**Revisado y aprobado por:** Firmado electrónicamente por: FRANCISCO XAVIER RODRIGUEZ GARZON Tngl. Francisco Rodríguez **DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (SUBROGANTE)**