PROCESO DE SELECCIÓN NIVEL 2 N° 003-2022 CMAC SANTA
"LICENCIAMIENTO DE ANTIVIRUS ENDPOINT, ANTISPAM Y SEGURIDAD PARA EQUIPOS EN TRABAJO REMOTO"

Chimbote, Marzo del 2022

I.- ESPECIFICACIONES TECNICAS REQUERIMIENTOS TÉCNICOS MÍNIMOS

1. REQUERIMIENTOS GENERALES

Que la **CMAC Santa SA** como entidad financiera líder en su rubro, adquiera una solución tecnología que corresponda a Antivirus Endpoint, Antispam y seguridad para equipos en Trabajo Remoto, con la finalidad de proteger todas las estaciones de trabajo, servidores, laptops y servidor de correos que forman parte de nuestra red interna, previniendo de manera proactiva cualquier infiltración de virus, spyware, troyanos, adwares, rootkits, phishing, spam y otros ataques.

2. REQUERIMIENTOS FUNCIONALES

2.1. REQUERIMIENTOS ESPECÍFICOS.

Descripción del Producto	Cantidad
Protección para Buzones de Correo – Exchange Server 2016	350
Protección de Equipos Locales (Estaciones de Trabajo) con Windows 7 y Superior (Inc. Trabajo Remoto).	300
Protección de Servidores Locales (Físico / Virtuales) con Windows Server 2003 – Superior	50
Protección de Equipos Legacy (Físico / Virtuales) – Windows XP	50

Se requiere que una empresa especializada en soluciones de seguridad informática, debidamente certificada por el fabricante, provea a nuestra institución la solución tecnología que corresponda a Antivirus Endpoint, Antispam y seguridad para equipos en Trabajo Remoto con la finalidad de salvaguardar de manera eficiente los datos de los equipos informáticos de la institución; por el periodo de un (01) año. Así mismo, que brinde el soporte y mantenimiento de la solución por todo el periodo del contrato.

CARACTERISTICAS DE LA SOLUCIÓN DE ANTIVIRUS PARA ESTACIONES DE TRABAJO:

- Deberá ser instalada para 300 estaciones de trabajo, donde el **PROVEEDOR** deberá desinstalar, si fuera el caso, cualquier antivirus existente en todas las estaciones de trabajo antes de instalar el antivirus propuesto, este trabajo se podrá realizar de manera remota con el personal de la **CMAC SANTA SA**.
- La licencia de seguridad de protección ofertada deberá ser capaz de ofrecer una completa protección antimalware avanzado para los Endpoints, dentro y fuera de la red corporativa, protegiendo contra virus, troyanos, gusanos, spyware, ransomware y nuevas variantes que puedan surgir.
- La Suite de Seguridad ofertada deberá estar presente en el último reporte de Gartner (2021) dentro del cuadrante de líderes para plataformas de protección Endpoint.
- Debe ofrecer prevención contra ataques de día cero y protección de vulnerabilidades nuevas y existentes para las estaciones de trabajo, deberá además bloquear los programas maliciosos para evitar que afecten una aplicación y suministrará firmas actualizadas automáticamente que protejan los equipos portátiles y de mesa frente a ataques, sin riesgo de probar y aplicar los paquetes de actualización de seguridad.

- La solución de seguridad ofertada deberá contar con una consola de gestión centralizada de tipo Software as a Service (SaaS) hospedada en la nube del fabricante de esta solución y poseer un agente para cada una de las estaciones de trabajo que permita observar de manera instantánea el estado de seguridad global y eventos específicos lo cual permitirá unificar el control de todas las herramientas de seguridad.
- El control de actualizaciones se realizará de manera incremental y automática desde la solución de seguridad.
- Con la plataforma integrada se permitirá bloquear los puertos de comunicación para combatir epidemias. Así como también crear políticas de denegación de escritura en forma centralizada para evitar la infección y propagación en la red, identificando y bloqueando inclusive botnets y ataques dirigidos de comunicaciones de comando y control (C&C) utilizando inteligencia de amenazas global y local.
- La solución deberá proveer detección y respuesta de amenazas automatizadas contra una variedad de amenazas de malware avanzadas, incluidos ataques sin archivos (fileless), cryptomining y ransomware.
- Capaz de proporcionar en un solo agente las siguientes características: prevención de pérdida de datos (DLP), control de aplicaciones, control de acceso a dispositivos, antimalware, etc.
- La solución deberá proveer las características de plataforma de protección de punto final (EPP) y Detección y respuesta de punto final (EDR) en un solo agente.
- Capaz de integrarse con la solución SIEM del cliente mediante syslogs
- Permita que los programas de terceros se integren con la solución a través de una interfaz de programación de aplicaciones (API)
- Debe tener un sistema de prevención de intrusiones (HIPS) basado en host para parchar virtualmente vulnerabilidades conocidas y desconocidas antes de que un parche esté disponible o desplegable.
- Fácil implementación del agente utilizando varios procedimientos compatibles (por ejemplo, instalación web, secuencia de comandos de inicio de sesión, paquete de instalación del agente, instalación remota de Windows, disco del cliente, Administrador de configuración de Microsoft System Center, etc.)
- La solución provee una consola de administración centralizada única para la administración más eficiente de todos los componentes de protección en el panorama de amenazas en constante cambio.
- La función de seguridad antimalware deberá estar integrada al mismo licenciamiento de la suite de seguridad, de tal manera que no requiera licencia adicional para cumplir con dicha funcionalidad.
- La solución de protección para estaciones finales deberá estar no solo basada en detección de firmas, sino también en comportamiento, heurística y reputación de archivos y web, basada en una nube probada dedicada a proteger proactivamente de malware, sea conocido en la base de firmas o sin estar contenido en ellas.
- Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros, de forma automática y en tiempo real.
- Cuando es descubierta una vulnerabilidad en el sistema operativo o en alguna aplicación, la solución deberá ser capaz de detener el ataque causado por el malware que aprovecha dicha vulnerabilidad, aun sin que exista un update/parche que solucione dicha vulnerabilidad.
- Detectar y proteger a las estaciones de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos.

- Manejar un sistema basado en distribución de firmas de malware desde la consola principal hacia las estaciones de trabajo, así como un sistema adicional de consulta de firmas de malware basado en reputación de archivos y reputación web.
- El sistema de firmas de malware basado en reputación de archivos podrá manejarse de manera integrada y visualizada desde la misma consola de antimalware. Asimismo, deberá manejar actualizaciones incrementales tanto del servidor hacia la nube, como del servidor hacia los clientes.
- La solución deberá contar con un sistema basado en la reputación de sitios Web que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo. El sistema de manejo deberá estar integrado en la misma consola de antimalware.
- Para aquellos programas válidos y que por su comportamiento el antimalware no permita su ejecución, deberá permitirlos agregándolos a una lista blanca.
- Los programas que no deben ser permitidos en la estación de trabajo, podrán ser agregados a una lista de bloqueo de programas específicos.
- Proporcionar o restringir el acceso a dispositivos de almacenamiento USB, CD/DVD y carpetas compartidas. La solución debe poder crear una lista blanca de dispositivos USB autorizados para su uso en la institución, así como para los dispositivos USB, CD/DVD y carpetas compartidas.
- El antimalware deberá permitir configurar que el usuario tenga permisos de control total, modificación, solo lectura, solo lectura y ejecución, o evitar que el usuario pueda tener acceso al contenido del dispositivo.
- La solución deberá poseer módulos de firewall e IDS/IPS, cuyo manejo debe estar integrado en la consola de administración de la solución. Esta debe ser capaz de permitir el bloqueo de puertos específicos y accesos indebidos que no estén en la tabla de políticas definidas por el administrador. Capaz de crear reglas de bloqueo/acceso para protocolos y aplicaciones. Protección proactiva contra ataques de "buffer overflow".
- Deberá tener capacidad de detectar y bloquear paquetes "exploit" que atacan vulnerabilidades de sistemas operativos Windows, aplicaciones comunes y bases de datos.
- La licencia debe ser capaz de prevenir el cifrado de archivos no autorizado como el creado por una infección tipo ransomware.

CARACTERÍSTICAS DE LA SOLUCIÓN DE ENCRIPTACIÓN PARA DISPOSITIVOS ENDPOINT

- La solución debe garantizar el cifrado de archivos, carpetas y medios extraíbles para 300 Endpoints.
- La consola de administración deberá ser implementada On-premise o en su defecto en un despliegue en nube, la **CMAC SANTA SA** sugiere que se realice en la nube tanto como sea posible.
- La solución debe tener integración con UEFI (Unified Extensible Firmware Interface), responsable de inicializar el hardware de los equipos antes de dar el control al sistema operativo.
- La solución debe contar con varios metodos de autenticación para el inicio de sesión en los equipos.
    - ColorCode: Una secuencia única de colores.
    - Domain Authentication: Sincronización LDAP de Active Directory para inicio de sesión único (SSO).
    - Fixed Password: Una cadena de caracteres, números y símbolos.
    - PIN: Un número de identificación personal estándar.

  - Remote Help: Autenticación interactiva para usuarios que olvidan sus credenciales o dispositivos que no tienen políticas sincronizadas dentro de un período de tiempo predeterminado.
  - Self Help: Combinaciones de preguntas y respuestas que permiten a los usuarios restablecer una contraseña olvidada sin ponerse en contacto con el Soporte técnico.
- La solución debe permitir el cifrado completo de disco incluyendo aplicaciones, configuraciones de registro, archivos temporales, archivos de intercambio, spoolers de impresión y archivos eliminados.
- La solución debe permitir a los usuarios restablecer una contraseña olvidada o una cuenta bloqueada antes de poder iniciar sesión el dispositivo.
- La solución debe contar con la certificación como mínimo de FIPS (Federal Information Processing Standard) 140-2 de Nivel 2, USB Implementers Forum (USB-IF) y Common Criteria Evaluation Assurance Level 4+.
- Sistemas operativos soportados: Windows 7, 8, 8,1 y 10; y macOS.

CARACTERÍSTICAS DE LA SOLUCIÓN DE ANTIVIRUS PARA SERVIDORES FÍSICOS Y/O VIRTUALES

- Deberá ser instalada para 100 servidores físicos y/o virtuales y sistemas operativos legacy como Windows XP, donde el PROVEEDOR deberá desinstalar, si fuera el caso, cualquier antivirus existente en todas las estaciones de trabajo antes de instalar el antivirus propuesto, este trabajo se podrá realizar de manera remota con el personal de la **CMAC SANTA SA**.
- La solución debe ser de tipo software as a Service (SaaS) hospedada en la nube del fabricante de esta solución y poseer un agente para cada uno de los servidores. Debe poder operar, al menos, en los siguientes sistemas operativos:
  - Plataformas de Servidores Microsoft Windows Server 2003 (32/64 bits) Windows Server 2003 R2 (32/64 bits), Windows Server 2008 (32/64 bits), Windows Server 2008 R2 (64 bits), Windows Server 2012 (64 bits), Windows Server 2012 R2 (64 bits), Windows Server Core 2012 (64 bits), Windows Server Core 2012 R2 (64 bits), y superiores.
  - Plataformas Linux RedHat Enterprise 5 (32/64 bits), RedHat Enterprise 6 (32/64 bits), RedHat Enterprise 7 (64 bits), Linux SUSE 11 (32/64 bits), Linux SUSE 12 (64 bits), CentOS 5 (32/64 bits), CentOS 6 (32/64 bits) CentOS 7 (64 bits), Ubuntu 14 (64 bits), Ubuntu 16 (64 bits).
  - Plataformas Legacy Windows XP.
  - Soporte para servidores alojados en plataforma de nube Azure y/o AWS
- La solución debe tener la capacidad reemplazar la solución antimalware y/o antivirus que actualmente use la institución, contando como mínimo módulos de Seguridad de: Antimalware, Servicio de reputación de archivos y/o URL, Análisis de Comportamiento y Machine Learning.
- Todas las actualizaciones del producto, de kernel, configuración y mantenimiento de la base de datos de seguridad deben estar a cargo del mismo fabricante.
- Deberá tener las características de protección contra código malicioso (Antimalware Avanzado):
  - La solución deberá contar con escaneos en tiempo real, escaneos programados y bajo demanda contra malware avanzado, virus y otros códigos maliciosos como son gusanos de red, spyware, troyanos, puertas traseras.
  - Los escaneos en tiempo real, escaneos programados y bajo demanda deben contar con la posibilidad de manejar excepciones por al menos tipos de archivos y rutas.
  - Deberá contar con la capacidad de envío de archivos infectados a cuarentena.

  - La solución deberá contar con una funcionalidad que le permita elegir la acción a tomar de manera automática dependiendo del tipo de amenaza detectada.
  - La solución deberá contar con la capacidad de aplicar al menos las siguientes acciones como limpieza, borrado y envío a cuarentena de archivo.
  - La solución debe contar con un cache para el escaneo en tiempo real y escaneos programados, a fin de optimizar el consumo de recursos en servidores virtuales.
  - La solución debe contar con la capacidad de integrar servicios de reputación del mismo fabricante, para mejorar la protección contra amenazas, debe contar con un servicio de reputación de archivos y un servicio de reputación de URL's.
  - El servicio de reputación de URL's evitará la conexión a sitios de mala reputación que puedan poner en riesgo la información que reside en los servidores de la institución.
  - El servicio de reputación de URL's debe configurarse mediante umbrales y debe permitir el manejo de excepciones.
- Deberá tener las características de protección de Análisis de Comportamiento y Aprendizaje Máquina:
  - La solución debe tener la funcionalidad de examinar elementos desconocidos a medida que se carguen y buscar comportamientos sospechosos en el sistema operativo, las aplicaciones y los scripts, detectar como interactúan para luego ejercer una acción de bloqueo.
  - La solución debe contar con la funcionalidad de analizar archivos desconocidos y amenazas de día cero mediante algoritmos de aprendizaje automático para determinar si el archivo es malicioso.

CARACTERÍSTICAS DE LA SOLUCIÓN DE DETECCIÓN Y RESPUESTA DE SERVIDORES Y ENDPOINT

- La solución deberá ser administrada desde una consola basada en nube y deberá estar licenciado para 300 estaciones de trabajo y 100 servidores.
- Ello con la finalidad de aprovechar de recursos no limitados de cómputo ofrecidos y administrado por el fabricante ofertado.
- La solución deberá brindar las capacidades de Detección y Respuesta de Servidores y Endpoint.
- Realizar investigación de amenazas a través del componente de la solución integrado en el agente desde la misma consola de administración centralizada.
- Debe tener un informe de análisis de causa raíz (RCA) visualizado.
- En la misma consola de gestión centralizada se deberá ver toda la información de amenazas y detección disponible, así como también realizar tareas de investigación como barridos de indicadores de compromiso (IOC), análisis de la causa principal y búsqueda de amenazas.
- La solución registrará los comportamientos del sistema, los comportamientos del usuario y las comunicaciones.
- Los datos de actividad, la telemetría de servidores y la recopilación de datos procedentes de estos servidores se enviarán al datalake del fabricante de la solución.
- Cuando se realiza una detección, los investigadores pueden buscar a través de los datos para analizar el impacto de la detección

CARACTERÍSTICAS DE LA SOLUCIÓN DE ANTISPAM

- Se deberá suministrar la solución de seguridad Antispam basada en nube para la protección de 350 buzones.
- La solución debe ser totalmente administrable por medio de una consola web en la nube
- La solución debe contar un 100% de disponibilidad en tiempo de actividad.
- La solución, al ser en la nube no se aceptará Appliance Virtual (VM) o que en su defecto, se requiera realizar una instalación invasiva sobre nuestro Exchange Server.
- La consola de administración deberá ser capaz de integrarse con microsoft active directory para la administración de usuarios y grupos.
- La consola debe mostrar gráficamente la pestaña Estadísticas principales de las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes relacionados con Business Email Compromise (BEC). (BEC) es un tipo de estafa dirigida a las empresas que realizan transferencias bancarias, las cuentas de correo electrónico corporativas, de ejecutivos, empleados de alto nivel relacionadas con finanzas o relacionadas con pagos de transferencias electrónicas son falsificadas y/o comprometidas mediante keyloggers o ataques de phishing para realizar transferencias fraudulentas, lo que resulta en cientos de miles de dólares en pérdidas.
- La consola debe tener la capacidad de mostrar la cantidad total de mensajes de correo electrónico escaneados por categoría detectada.
- La consola debe mostrar en detalle la cantidad de mensajes detectados como ransomware.
- La consola debe mostrar gráficamente las amenazas y el porcentaje total de mensajes detectados como amenaza.
- La consola deberá contar con espacios independientes para la administración de políticas de protección tanto de entrada como de salida.
- La consola debe mostrar las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes que contienen amenazas avanzadas, malware, spam.
- La solución debe permitir la configuración de políticas para comunicación cifrada.
- La consola debe hacer trazabilidad de Time-of-Click realizado a las URL´s y la acción realizada por la solución. La disponibilidad del servicio de Time-of-Click debe detectar malware basado en enlaces y ataques de phishing al analizar la reputación de una URL al momento del clic de los usuarios y no solo en el momento de la entrega a del email.
- La consola debe enviar las notificaciones de las alertas generadas vía correo electrónico.
- La solución debe permitir crear reglas específicas que tomen medidas sobre tipos de mensajes potencialmente no deseados como Spam, Phishing, Graymail, Reputación Web o Ingeniería social.
- La solución debe permitir la creación reglas específicas que tengan acciones en mensajes que contienen malware, gusanos, troyanos u otro código malicioso.
- La solución debe permitir importar y exportar los remitentes, los destinatarios y las listas de excepciones para las reglas de política tanto en la protección de entrada como de salida.
- La consola debe dar la opción de crear y administrar listas de remitentes bloqueados y aprobados.
- La solución deberá utilizar una combinación de exploración basada en patrones y heurística para detectar explotaciones de documentos y otras amenazas utilizadas en ataques dirigidos.
- La solución debe permitir al usuario final administrar su propia consola de correos en cuarentena.

- La solución deberá permitir la configuración del Inicio de Sesión Único (SSO) para los usuarios de la consola de cuarentena mediante un Servidor de Federación (Microsoft Active Directory Federation Services (AD FS) 2.0 y Azure Active Directory (AD)).
- La solución debe permitir la administración de Graymail (mensajes de correo electrónico masivos solicitados que no son spam) por separado del spam.
- La solución debe ser 100 % compatible de para la protección en nube con Microsoft Exchange, Microsoft® Office 365 y Google Gmail.
- Debe cumplir como mínimo las siguientes características relacionados a Compliance:
    - La solución debe contar con certificaciones de privacidad de datos como ISO 9001, ISO 27001 y SAS 70 Type II.
    - La solución no puede superar una latencia de un minuto en la entrega del correo electrónico.
    - La asistencia técnica debe estar disponible para de forma ininterrumpida por correo electrónico o por teléfono.
    - Se debe proporcionar compatibilidad con el cumplimiento de GDPR en plantillas de prevención de pérdida de datos (DLP).
    - La solución debe tener un sistema de validación para detectar y evitar la suplantación de correo electrónico.
    - La solución deberá contar con DLP, con el fin de proteger la pérdida de datos mediante el control del tráfico de correo saliente.
- Debe contemplar reportes que cuenten con las siguientes características:
    - La solución permite la generación de reportes bajo demanda o calendarizados.
    - La solución debe tener un módulo de registros de auditoría que permita rastrear la administración y los eventos ocurridos.
    - La consola deberá mostrar la cantidad total de mensajes aceptados y bloqueados junto con su porcentaje total en un rango de fechas especifico.

2.2. SERVICIOS REQUERIDOS

El **PROVEEDOR** deberá de cumplir con los siguientes entregables:

Entregable	Periodicidad y Fecha de Entrega
SLA donde se incluya los correos, teléfonos y niveles de escalamiento (Incluir Proceso) para la atención de soporte o incidencia.	Una ocasión, a más tardar, 2 días hábiles posteriores al inicio de la vigencia del servicio.
Reporte del resumen del estado de seguridad de servidores y estaciones de trabajo, se debe de incluir lo siguiente: - Detalle de versiones Instaladas. - Detalle de equipos actualizados y desactualizados. - Detalle de equipos sin antivirus. - Detalle de equipos con ataque de red. - Detalle de equipos con licenciamiento utilizado. El reporte deberá demostrar al menos los siguientes campos: Nombre de Host, Número de IP, Versiones, Datos de IP Atacante.	Semanal, durante la vigencia del servicio. A más tardar los viernes hasta el termino de contrato.

- El **PROVEEDOR** deberá de realizar la capacitación sobre la solución instalada en el entorno **CMAC SANTA SA** y deberá de brindar el Know-How necesario para poder administrar la plataforma.

3. REQUERIMIENTOS NO FUNCIONALES

El **PROVEEDOR** deberá de presentar una carta de fabricante donde se exprese que es un distribuidor autorizado por la marca. Así mismo, deberá evidenciar que cuenta con el personal técnico calificado y certificado (en planilla y no terceros) para proveer los servicios que la **CMAC SANTA SA** está solicitando.

El **PROVEEDOR** deberá de evidenciar que cuenta con una Mesa de Ayuda 7x24x365 y que es responsable directo (no terceros).

3.1. CARACTERISTICAS DEL PROVEEDOR

- Durante el período de garantía comercial, el **PROVEEDOR** debe contar con un Centro de Operaciones de Seguridad para el servicio de Soporte Técnico 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los tickets de cambios de configuraciones de políticas en el dispositivo de seguridad.
- El postor deberá contar con un Centro de Operaciones de Seguridad (SOC) certificado en ISO 27001 para el servicio de Soporte Técnico, con la finalidad de garantizar que se cuente con procesos de atención óptimos que asegure el cumplimiento de los tiempos de respuesta, la calidad de su atención, así como el aseguramiento de la confidencialidad e integridad del manejo de los datos y de la información de la entidad.
- El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará "falla".
- El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".
- El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.
- Deberá brindar soporte técnico In Situ a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá a la ENTIDAD en forma personal. Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota.
- El **PROVEEDOR** deberá garantizar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y de activar un plan de contingencia cuando una falla se produzca.
- El servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda del **PROVEEDOR**, registrará el requerimiento y/o falla del servicio y proporcionará un número de ticket.
- El servicio de soporte técnico incluirá un servicio de monitoreo y gestión de incidencias para la plataforma ofertada, el cual deberá cumplir los siguientes requisitos mínimamente:
- Brindar una capa de SIEM para la retención de logs, mínimo de 90 días.
- Brindar capas adicionales, como analítica de comportamiento de usuarios (UBA), orquestación, automatización y respuesta de seguridad (SOAR), Data Lake para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio, sin costo adicional.

- Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el **PROVEEDOR** deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones.
- El portal debe actuar como un front-end independiente de la capa tecnológica descrita en los puntos anteriores (SIEM, UBA, SOAR, data lake, I.A.).
- El portal deberá mostrar investigaciones por el periodo de contrato para efectos de historial y permitir consultas como: fecha de creación, fecha de resolución, fuentes datos, estados, por lo menos 3 niveles de condición de defensa o DEFCON (normal, intermedio y critica) asociado a las investigaciones y misiones pendientes de revisar.
- Las investigaciones presentadas en el portal deberán incluir información del estado, tipo, analista asignado, fuente de datos asociada y si existen misiones (debe permitir notificar cualquier modificación del estado). Deberá también mostrar un resumen de la investigación detallando lo ocurrido, magnitud, conclusión y una sección donde se deberá incluir evidencia como archivos o indicadores. Finalmente, deberá mostrar una línea de tiempo con actividades asociadas a la investigación, así como las interacciones entre analistas de seguridad.
- Monitoreo 24x7 identificando amenazas cibernéticas que puedan afectar la operación.
- Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes, CERT y Dark Web. Las fuentes de inteligencia de amenazas deberán ser enviadas al SIEM para correlacionar y generar detecciones. El **PROVEEDOR** deberá adjuntar a su propuesta técnica un listado de fuentes de inteligencia (mínimo 10) con las que operan.
- Caza de amenazas sobre el SIEM, identificando, evaluando y mejorando la capacidad de detección mediante búsqueda exhaustiva de ciber-amenazas y actividades maliciosas.
- Respuesta y mitigación de incidentes en tiempo real ante ciber-amenazas.
- Optimización de procesos consistentes de desarrollo y aprendizaje que incluyan optimización de reglas, actualizaciones y sugerencias de implementación de nuevas tecnologías de detección de amenazas cibernéticas.
- Investigación forense de procesos en curso de presuntas actividades maliciosas y amenazas cibernéticas incluyendo el análisis post mortem de incidentes verificados. Mínimo de 4 horas mensuales de ser requerido.
- La solución deberá procesar logs de por lo menos 700 fuentes de datos en nube y locales. En caso no exista una integración, sin costo adicional, se deberá poder crear una personalización en no más de 90 días desde la solicitud y dentro del alcance del requerimiento.
- Envío periódico de IOC del tipo email, dominio, URL, sha3-256, IP, MD5, SHA1 y SHA256 en formato STIX.
- Brindar una llave API y URL para digerir los IOC de forma automática.

4. **NIVELES DE SERVICIO.**

El **PROVEEDOR** se compromete a brindar soporte técnico y mesa de ayuda en 7x24x365, por el periodo de 1 año de manera remota.

Tiempo de respuesta: El tiempo de respuesta sugerido por la **CMAC SANTA SA** es el siguiente.

- Severidad 1 – Critica: < 1 Hora.
- Severidad 2 – Alto: 2 Horas.
- Severidad 3 – Medio: 4 Horas.

- Severidad 4 – Bajo: 8 Horas.

Tiempo de seguimiento: El tiempo de seguimiento esperado por la **CMAC SANTA SA** es el siguiente.

- Severidad 1 – Critica: Cada 2 horas hasta que se resuelva o se aplique un Workaround.
- Severidad 2 – Alta: Cada 24 Horas hasta que se resuelva o se aplique un Workaround.
- Severidad 3 – Medio: Cada 2 días laborales hasta que se resuelva.
- Severidad 4 – Bajo: Semanalmente hasta que se resuelva.

Definición de Severidad:

- Critica: El producto no funciona y afecta críticamente al entorno de producción. No existe Workaround disponible.
- Alta: El producto está deteriorado y el entorno de producción de cliente funciona con deficiencias. No existe Workaround disponible.
- Media: Una función del producto ha fallado y no se ve afectado el entorno de producción. El servicio de soporte lo conoce y existe un Workaround disponible.
- Baja: El funcionamiento del producto no se ve afectad y sin impacto en el negocio del cliente. Incluye información, documentación procedimiento y solicitudes de mejora por parte del **PROVEEDOR.**

5. **CRONOGRAMA DE ACTIVIDADES.**

El **PROVEEDOR** deberá de cumplir con el plan de trabajo previamente acordado con el personal técnico de la **CMAC SANTA SA**, a través del Departamento de Sistemas y Procesos.

El **PROVEEDOR** deberá de presentar en su propuesta, un cronograma de actividades para la implementación y puesta en marcha de "**LICENCIAMIENTO DE ANTIVIRUS ENDPOINT, ANTISPAM Y SEGURIDAD PARA EQUIPOS EN TRABAJO REMOTO**", considerando que la fecha de inicio y fecha de fin no debe de impactar en la productividad de la **CMAC SANTA SA.**

6. **PERSONAL CLAVE.**

- **Jefe del Proyecto**
  - Un (01) Profesional titulado en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones; deberá estar colegiado y habilitado al momento de la presentación de la propuesta.
  - Deberá contar con certificación del Project Management Professional (PMP) vigente.
  - Deberá contar con experiencia mínima de tres (03) años en Gestión de Proyectos de TI.
- **Especialista de Seguridad**
  - Un (01) Especialista en Seguridad con certificación vigente del fabricante de la solución ofertada.
  - Deberá contar con experiencia mínima de dos (02) años en la implementación y/o soporte de soluciones de seguridad de protección de puntos finales.

7. **INFORMACIÓN ADICIONAL.**

El **PROVEEDOR** deberá de brindar un entrenamiento técnico constante para dos personas del departamento de sistemas y procesos con la finalidad de poder realizar la administración, instalación, mantenimiento y configuración sobre el producto de manera eficiente. Esta capacitación se debe de realizar de la siguiente manera:

- Capacitación técnica al inicio de realizar el licenciamiento y explicar detalladamente el funcionamiento de la consola, esta capacitación se deberá de realizar de manera remota.
- Cualquier ticket de soporte abierto y solucionado por el **PROVEEDOR**, este deberá de brindar una guía y una explicación por MS Teams, Zoom u otro medio conectado a la consola.
- Dos capacitaciones adicionales de al menos 4 horas al año para habilitar nuevas características del producto.

II.-VALOR REFERENCIAL:

S/ 95,000.00 Soles (Noventa y cinco mil con 00/100 Soles) lo cual incluye impuestos y todos los gastos que se generen para la instalación y ejecución. Las propuestas que exceden el valor referencial serán consideradas no válidas.

III.- CRONOGRAMA DEL PROCESO:

ETAPA	FECHA
Convocatoria	Del 01/03/2022 al 02/03/2022
Presentación de Propuestas	03/03/2022
Evaluación, Calificación y Elección de la Propuesta Ganadora	04/03/2021
Buena Pro	04/03/2021

IV.- PRESENTACION DE PROPUESTAS:

Las propuestas se presentarán por medio electrónico en la fecha señalada en el cronograma, a los emails pbermudez@cajadelsanta.pe con copia a los emails eperalta@cajadelsanta.pe ; mvalle@cajadelsanta.pe Los archivos de las propuestas deben ir con clave. La clave la enviarán el día 04 de marzo a las 9:00 a.m. a los email de pbermudez@cajadelsanta.pe y eperalta@cajadelsanta.pe La evaluación la realizarán los funcionarios responsables en acto privado.

Para que una propuesta sea admitida deberá contener los documentos solicitados en las especificaciones técnicas (carta de la marca, SLA, declaraciones juradas, documentación del personal clave, etc) ; así como los términos de referencia indicados.

La toma de conocimiento, en cualquier etapa del proceso y hasta antes de la suscripción del contrato, de la existencia de antecedentes negativos evidenciados que pudiera tener el postor y cualquiera de sus representantes o personas vinculadas a aquel, que lo relacione con la investigación o comisión de algún ilícito penal así como la trasgresión de cualquiera de los

principios rectores, valores y políticas que regulan la buena marcha institucional, conforme a las normas de prevención vigentes, de tal forma que haga insostenible la relación comercial con la empresa, debido al alto riesgo de pérdida patrimonial o reputacional, será causal de considerar nula la participación del respectivo postor, en forma automática.

INDISPENSABLE:

- Inscribirse como proveedor , llenando las fichas del Anexo N° 01, el cual debe ser remitido al email pbermudez@cajadelsanta.pe el día 02 de marzo 2022.

  Para la inclusión en el registro de proveedores de la entidad, las personas naturales y personas jurídicas deben seguir lo estipulado a continuación:

  1.Contar con RUC activo y habido. Adjuntar Ficha RUC.
  2. No deberá registrar deudas vencidas en el sistema financiero, informadas en central(es) de riesgo con un periodo no menor de tres (03) meses con calificación 100% Normal.
  3. No registrar deuda en cobranza coactiva en SUNAT.
  4. No registrar antecedentes penales ni judiciales (presentar declaraciones juradas) ni estar vinculados a investigaciones o procesos por la comisión de ilícitos penales incompatibles con la naturaleza de la prestación que ofrece el proveedor, a criterio de la entidad. Esta disposición alcanza a las personas naturales y a los representantes de las personas jurídicas que desean incluirse en el registro de proveedores de la entidad.
  5. No estar inhabilitado a contratar con el Estado.
  6. No pertenecer a la lista negativa de acuerdo a los lineamientos de Prevención de lavado de activos y del financiamiento del terrorismo establecidos por la entidad.

EVALUACIÓN DE PROVEEDORES:

<table>
<tr><th>Evaluación Técnica</th><th>Puntaje</th></tr>
<tr><td>Cumplimiento del Requerimiento Técnico</td><td>40</td></tr>
<tr><td>Tiempo de Implementación e Instalación
<table>
<tr><th>Tiempo de Instalación</th><th>Puntaje</th></tr>
<tr><td>Hasta 30 días</td><td>30 puntos</td></tr>
<tr><td>Hasta 45 días</td><td>20 puntos</td></tr>
</table>
</td><td>30</td></tr>
<tr><td>Experiencia comprobada en Seguridad Informática (como Soluciones de Proteccion de Puntos Finales y Seguridad Perimetral en general) mínima de 3 Años, acreditando con contratos u órdenes de compra o servicios y su respectiva constancias de conformidad de servicio. Presentar Anexo 04 y copias de los contratos, ordenes de compra/servicio y conformidad del servicio</td><td>20</td></tr>
<tr><td>Curso de Visual Studio 2019 Developer (Online) – 01 Persona</td><td>10</td></tr>
</table>

Para pasar a la oferta económica el postor deberá alcanzar un puntaje mínimo de 70 puntos.

Evaluación Económica	$P_i = O_m \times 100 / O_i$
Consistirá en asignar el puntaje máximo establecido (100) a la propuesta económica de menor monto. Al resto de propuestas se les asignará un puntaje inversamente proporcional.	i = Propuesta P_i = Puntaje de la propuesta económica i O_i = Propuesta económica i O_m = Propuesta económica de monto/precio más bajo

PUNTAJE TOTAL:

Una vez calificadas las propuestas mediante la evaluación técnica y económica se determinará el puntaje total de las mismas.

El puntaje total de la propuesta será el promedio ponderado de ambas evaluaciones, obtenido de la siguiente fórmula:

PTPi = c1 PTi + c2 PEi

Donde:

PTPi = Costo Total del postor i
PTi = Puntaje de la evaluación técnica del postor i
PEi = Puntaje de la evaluación económica del postor i
c1 = Coeficiente de ponderación para la evaluación técnica = 0.60
c2 = Coeficiente de ponderación para la evaluación económica = 0.40

CALIDAD:

La calidad debe entenderse como el cumplimiento estricto de las especificaciones técnicas.

CONFORMIDAD DE LA ENTREGA:

La conformidad de las licencias estará a cargo de la oficina directamente comprometida (área usuaria), en un plazo que no excederá de uno (1) a cinco (05) días calendarios de recibido el producto.

FORMA DE PAGO:

Son requisitos de pago los siguientes:

- Que la empresa proveedora haya cumplido con la remisión de la factura correspondiente, según las condiciones establecidas en la Orden de Compra respectiva.

El expediente completo de pago deberá incluir:

- Comprobante de pago (USUARIO y SUNAT) en Original y en Fotocopia.
- Copia de la Orden de Compra debidamente firmado.
- Carta de autorización para el caso de abonos en cuenta.

ANEXO N° 01

DECLARACIÓN JURADA DE DATOS PARA LA INSCRIPCIÓN COMO PROVEEDOR Y/O CONTRAPARTE DE LA CMAC SANTA

Señores
Caja Municipal de Ahorro y Crédito del Santa S.A.
Dpto. de Logística
Chimbote. -

Estimados señores:

El(la) que se suscribe, ……, identificado(a) con DNI Nº ....., en representación de la empresa ……., con RUC N°……; se presenta ante vuestra representada brindando la siguiente información:

DATOS DEL PROVEEDOR Y/O CONTRAPARTE			
Apellidos y Nombres / Razón Social:			
Tipo Documento:		*Nº Documento:*	
Dirección:		*Ciudad:*	
Teléfono(s):		*Años de experiencia:*	
E-mail:		*Página Web:*	
CONTACTO RESPONSABLE			
Apellidos y Nombres:		*Nº DNI:*	
E-mail:		*Nº Celular:*	

IDENTIFICACION DE LOS ACCIONISTAS / SOCIOS / ASOCIADOS		
Apellidos y Nombres	***N° Documento***	***Cargo***

RUBROS EN LOS QUE EL PROVEEDOR Y/O CONTRAPARTE BRINDA SUS PRODUCTOS O SERVICIOS

……., ……. de……. del 20…….

_____
Firma y/o Sello del Proveedor o Contraparte

DECLARACIÓN JURADA DEL PROVEEDOR Y/O CONTRAPARTE

El (la) que suscribe ……..…… identificado con DNI Nº ……..……, representante de la Empresa ……..., identificada con RUC Nº……, Declaro Bajo Juramento lo siguiente:

- Cuento con RUC Activo
- No registro deudas vencidas en el sistema financiero, registradas en central(es) de riesgos.
- No registro deuda en cobranza coactiva en SUNAT.
- No Registro antecedentes penales, judiciales, así como no estar inmerso en delito de lavado de activos (Esta disposición alcanza a las personas naturales y a los representantes de las personas jurídicas que desean incluirse en el Registro de Proveedores de la Caja).
- No estar inhabilitado a contratar con el Estado.

……..……, ……. de……..…… del 20……

Firma y/o Sello del Proveedor o Contraparte

ANEXO N° 02

CARTA DE PROPUESTA ECONOMICA
(MODELO)

Señores:
Departamento de Logística.

Proceso Nivel 2 N° 003-2022 CMAC SANTA
"LICENCIAMIENTO DE ANTIVIRUS ENDPOINT, ANTISPAM Y SEGURIDAD PARA EQUIPOS EN TRABAJO REMOTO"

Presente.-

De nuestra consideración,

A continuación, hacemos de conocimiento que nuestra propuesta económica es la siguiente:

Descripción del Producto	PRECIO UNITARIO	PRECIO TOTAL

El monto total de nuestra oferta asciende a……..

El valor de la propuesta incluye todos los tributos, seguros, transportes, inspecciones, costos laborales, conforme a la legislación vigente, así como cualquier otro costo que pueda tener incidencia sobre el costo del bien y/o servicio a contratar.

Chimbote,……

……
Firma, Nombre / Razón social del postor

ANEXO N° 03

DECLARACIÓN JURADA DE OFERTA DE PLAZO DE INSTALACION

Proceso Nivel 2 N° 003-2021 CMAC SANTA
"LICENCIAMIENTO DE ANTIVIRUS ENDPOINT, ANTISPAM Y SEGURIDAD PARA EQUIPOS EN TRABAJO REMOTO"

El que se suscribe, don ……, identificado con DNI Nº..... Representante Legal de....., con RUC. Nº …… **DECLARO BAJO JURAMENTO** que con respecto a los bienes materia del presente proceso de selección que mi oferta es la siguiente:

PLAZO DE INSTALACION (DIAS)	

Lugar, ……..

……..……..
Firma y sello del representante legal
Nombre / Razón social del postor

ANEXO N° 04

EXPERIENCIA DEL POSTOR

Señores:
CMAC SANTA S.A.
PROCESO DE SELECCIÓN NIVEL 2 N° 003-2022-CMAC-S: "LICENCIAMIENTO DE ANTIVIRUS ENDPOINT, ANTISPAM Y SEGURIDAD PARA EQUIPOS EN TRABAJO REMOTO".
Presente.-

El que suscribe....., con DNI N°....., Representante Legal de la Empresa.....
con RUC. N°....., y con Domicilio Legal en....., detallamos lo siguiente:

N°	CLIENTE	OBJETO DEL CONTRATO U ORDEN DE COMPRA/SERVICIO	N° CONTRATO U ORDEN DE COMPRA / SERVICIO	IMPORTE DEL CONTRATO U ORDEN DE COMPRA/SERVICIO	FECHA DE INICIO Y TÉRMINO
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
	TOTAL				

<Lugar>, ***<día>*** de ***<mes>*** del ***<año>***

La información debe ser complementada con copia de los contratos , ordenes de compra y conformidades de servicio