

CONTRATO ELECTRÓNICO DE PRESTACIÓN DE SERVICIOS N° SAMC-004-2024 CELEBRADO ENTRE LA CAJA DE RETIRO DE LAS FUERZAS MILITARES CON NIT. 899.999.118 – 1 Y UT CREMIL 2023 IDENTIFICADA CON NIT N°901.783.613 – 2

Entre los suscritos, **Coronel (RA) FREDY HERNÁN CALIXTO MONROY**, mayor de edad y vecino de esta ciudad, identificado con cédula de ciudadanía No. 79.548.026 de Bogotá D.C., quien obra en calidad de Subdirector Administrativo de la **CAJA DE RETIRO DE LAS FUERZAS MILITARES CREMIL** – nombrado para el cargo mediante Resolución No. 2767 del 13 de marzo de 2020, delegado para contratar hasta por 1.000 S.M.M.L.V según Resolución No. 15848 de 2018, quien en adelante se denominará **LA CAJA**, por una parte y por la otra UT CREMIL 2023 identificada con NIT 901.783.613-2 e integrada por la empresa DATAMOTION S.A.S identificada con NIT. 901.477.680-4 representada legalmente por Andrea Palacios Villamizar – SIGLA-DATAMOTION SAS identificada con cedula de ciudadanía N° 1.018.408.058 expedida en Bogotá D.C con un PORCENTAJE DE PARTICIPACIÓN 80%, y por la empresa CAPACITACIÓN Y SERVICIOS ESPECIALIZADOS S.A.S – SIGLA- CAYSES S.A.S identificada con NIT. No. 830.110.359-1 representada legalmente por el señor Sergio Serrano Galvis identificado con cedula de ciudadanía N° 91.279.828 expedida en Bucaramanga – Santander PORCENTAJE DE PARTICIPACIÓN: 20%, quien en adelante se denominará **EL CONTRATISTA**, hemos acordado celebrar el presente contrato electrónico de prestación de servicios, previas las siguientes consideraciones: A) Que la Caja de Retiro de las Fuerzas Militares adelantó un Proceso de Selección Abreviada de Menor Cuantía SAMC-004-2024. B) Que mediante Resolución N° 6401 del 16 de Julio de 2024 la Entidad dispuso la apertura del proceso de Selección Abreviada de Menor Cuantía SAMC-004-2024. C) Que el día 08 de agosto de 2024 se realizó el cierre del proceso, conforme consta en la lista de ofertas publicada en el portal de contratación SECOP II, con un total de 2 ofertas. D) Que teniendo en cuenta la evaluación definitiva, mediante Resolución N° 7087 del 30 de agosto de 2024 la Entidad adjudicó el proceso. E) Que el contrato que se celebra se rige de acuerdo con lo establecido en la Ley 80 de 1993, Ley 1150 de 2007, Decreto 1082 de 2015 y en lo no regulado, por las disposiciones de la Ley Civil y Comercial y se rige por las siguientes:

CLÁUSULA PRIMERA- OBJETO: “CONTRATAR LA ADQUISICIÓN DE UN SOFTWARE ANTIVIRUS ORIENTADO A XDR (ENDPOINT) Y LA RENOVACIÓN DE LA SUSCRIPCIÓN DE UNA HERRAMIENTA DE SEGURIDAD CON EL SERVICIO DE SOPORTE TÉCNICO DE FABRICA Y LOCAL PARA LA CAJA DE RETIRO DE LAS FUERZAS MILITARES.”

CLÁUSULA SEGUNDA- OBLIGACIONES GENERALES DEL CONTRATISTA: 1. Cumplir oportunamente con el contrato en los términos y condiciones establecidas en el mismo. 2. Ejecutar idónea y eficazmente el objeto del contrato y las obligaciones inherentes. 3. Constituir las garantías pactadas en el contrato dentro del término establecido. 4. Suscribir acta de inicio con el supervisor del contrato. 5. Cumplir con el objeto del contrato con plena autonomía técnica y administrativa y bajo su propia responsabilidad. Por lo tanto, no existe ni existirá ningún tipo de subordinación, ni vínculo laboral ni de otra índole con la Caja de Retiro de las Fuerzas Militares, por lo que cada contratista asumirá el pago de aportes a la seguridad social, de acuerdo con la normatividad vigente. 6. Cumplir las obligaciones con el Sistema de Seguridad Social Integral y presentar los documentos respectivos que así lo acrediten, conforme lo establecido por el artículo 50 de la Ley 789 de 2002, las Leyes 828 de 2003, 1122 de 2007 y 1562 de 2012, los Decretos 1703 de 2002 y 510 de 2003, el artículo 23 de la Ley 1150 de 2007 y las demás normas que las adicionen, complementen o modifiquen 7. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y en trabamientos que puedan presentarse. 8. Participar y apoyar a CREMIL en todas las reuniones a las que éste lo convoque relacionadas con la ejecución del contrato. 9. Reportar cualquier novedad o anomalía que se presente en el desarrollo del contrato al supervisor del contrato. 10. Mantener la reserva profesional sobre la información que le sea suministrada para la ejecución del objeto del contrato, garantizando así la estricta confidencialidad, seguridad, inviolabilidad e imposibilidad de filtración de la información, fuga o salida de material de la Caja. 11. Responder por sus actuaciones y omisiones derivadas de la celebración del presente contrato, y de la ejecución de este. 12.

Informar por escrito al supervisor del contrato sobre las actividades desarrolladas, que tengan relación con el objeto contratado. **13.** Acatar las instrucciones que imparta CREMIL para el cumplimiento del contrato a través del supervisor de este. **14.** Permitir, facilitar, disponer, atender con prontitud los requerimientos de información, recomendaciones, y solicitudes que adelante la Caja. **15.** Mantener niveles de eficiencia técnica y profesional para cumplir sus obligaciones contractuales y ejercer permanentemente autocontrol a las actividades, procesos, procedimientos y productos que se deban ejecutar y realizar para el efecto. **16.** Elaborar y Presentar informes que le sean solicitados por el supervisor del contrato. **17.** Entregar al supervisor designado la información que se requiera para la verificación y seguimiento de las actividades que se llevan a cabo dentro del presente contrato. **18.** Presentarse a la Caja en el momento en que sea requerido por el supervisor del contrato para la suscripción de la correspondiente acta de liquidación. **19.** Cumplir con la normatividad del Decreto 1072 de 2015 y resolución 0312 del 2019 en cuanto Seguridad y Salud en el trabajo y acatar los requisitos legales de aspectos e impactos ambientales. (política del Sistema Integral de Gestión, objetivos, EPP adecuados según la tarea a ejecutar, matriz de identificación de peligros y aspectos e impactos ambientales). **20.** Entregar CREMIL una vez finalizado la ejecución del contrato toda la información y los documentos recopilados en desarrollo para el cumplimiento de sus obligaciones, de conformidad con las normas y disposiciones vigentes en el MEN, debidamente escaneadas **21.** Las demás obligaciones, que le sean asignadas por el supervisor de la naturaleza del objeto del contrato.

CLÁUSULA TERCERA: OBLIGACIONES ESPECIFICAS DEL CONTRATISTA: el CONTRATISTA se compromete a cumplir con las siguientes obligaciones Especificas: **1.** Cumplir con el objeto del contrato y las especificaciones incluidas en el anexo técnico, el cual hace parte integral del mismo. **2.** Presentar cronograma de trabajo con las actividades a realizar para la puesta en marcha de los servicios contratados dentro de los cinco (5) días siguientes al perfeccionamiento del contrato. El cronograma deberá estar ajustado al plazo de ejecución del contrato. **3.** Suscribir con el supervisor del contrato el acta de inicio, con los anexos solicitados en el anexo técnico y en el estudio previo, los cuales hacen parte integral del mismo. **4.** Identificación y evaluación de amenazas y vulnerabilidades. **5.** Elaboración de informes detallados sobre los riesgos identificados basado en OSSTMM **6.** El contratista deberá realizar políticas y procedimientos de seguridad adaptados a las necesidades del Grupo de Informática. **7.** El contratista deberá generar Informes periódicos de Vulnerabilidades **8.** Establecimiento de sistemas de monitoreo en tiempo real. **9.** Configuración de alertas para eventos de seguridad críticos. **10.** Sesiones de formación periódicas sobre prácticas seguras en el uso de sistemas informáticos. **11.** Acompañamiento al oficial de Seguridad en el cierre de los análisis de Vulnerabilidades. **12.** Evaluación continua de las vulnerabilidades y aplicación de soluciones. **13.** El contratista deberá realizar asesoramiento al grupo de informática en actividades de ciberseguridad **14.** Debe tener la capacidad de evaluar el riesgo y priorizar las acciones para remediar las vulnerabilidades y cubrir los vectores de ataque. **15.** Poder realizar escaneos periódicos (al menos uno mensualmente) con el fin de comparar con los resultados históricos y detectar cambios recientes. **16.** Sugerir acciones que sirvan de bases para remediar los problemas identificados **17.** Soportar herramientas orientadas a la protección del buen nombre de La Entidad. **18.** Soportar el uso de algoritmos para detectar ataques de tipo 'Typosquatting', con el fin de monitorear nombres de dominio similares al de La Entidad. **19.** Debe tener soporte para el monitoreo de credenciales que hayan sido filtradas/expuestas en internet. **20.** Soportar el monitoreo de aplicaciones móviles no autorizadas por La Entidad. **21.** Soportar el monitoreo de discusiones en redes sociales que vayan en contra de la reputación de La Entidad. **22.** Debe tener la capacidad de identificación técnicas comunes de suplantación de marca en redes sociales. **23.** Soportar la configuración del monitoreo y seguimiento de campañas de 'phishing' en contra de La Entidad. **24.** Debe soportar realizar la eliminación (takedown) ya sea de sitios web o aplicaciones no autorizadas. **25.** Identificar fugas sensibles de código fuente propiedad de La Entidad. **26.** Identificar buckets de almacenamiento abiertos en la nube. **27.** Suministrar información contextual sobre amenazas inminentes para La Entidad.

CLÁUSULA CUARTA: - OBLIGACIONES DEL CONTRATANTE: **1.** Cumplir con lo estipulado por la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011 y el Decreto 1082 de 2015. **2.** Suministrar al contratista la información que se requiera para el cumplimiento del objeto contractual. **3.** Informar oportunamente al

contratista sobre cualquier decisión administrativa que tenga incidencia en el objeto del contrato. **4.** Pagar oportunamente en las condiciones pactadas. **5.** Supervisar el contrato según la Ley 1474 de 2011.

CLÁUSULA QUINTA: - ESPECIFICACIONES TÉCNICAS

- Renovar la suscripción de la herramienta de gestión de vulnerabilidades TENABLE.IO (Vulnerability Management) para 1000 esst
- Suministro, instalación y configuración de una herramienta antivirus orientado a XDR endpoint
- Servicio de soporte técnico con fabricante y local 7x24 por un (1) año

El contratista deberá desarrollar el cumplimiento de las siguientes actividades para la adquisición y renovación de las herramientas de seguridad para garantizar la continuidad y disponibilidad del servicio y cumplir con los criterios de administración, gestión, mantenimiento y soporte así:

A	DESCRIPCION TECNICA DEL BIEN Y/O SERVICIO A RENOVAR
1	Renovación suscripción tenable.IO para 1000 esst (activos)
2	La plataforma se maneja desde la nube
3	La cantidad de los dispositivos a escanear entre PC, servidores, sitios web, dispositivos de red, demás dispositivos, etc., serán definidos desde el inicio de la ejecución del contrato con el supervisor.

1	SISTEMA DE ANÁLISIS DE VULNERABILIDADES – TENABLE PARA 1000 ESST
1.1	El servicio contratado deberá estar licenciado con garantía de fábrica, gestionado y soportado localmente por un (1) año desde el inicio de la ejecución del contrato.
1.2	La suscripción debe estar a nombre de Caja de retiro de las FF.MM, correo: informatica@cremil.gov.co
1.3	Monitoreo permanente de la plataforma tenable como resultado de los escaneos y análisis de vulnerabilidades generando informes periódicos basados en vistas personalizadas (p. Ej., especificar tipos de vulnerabilidades, por host / por usuario /por servidores / por sitios web, etc), definición de formatos (HTML, CSV, XML), de manera semanal y/o mensuales concertadas con el supervisor del contrato.
1.4	Realizar escaneo de vulnerabilidades de manera periódica, una vez detectadas se deben generar sesiones de trabajo con el contratista quien hará el acompañamiento en la remediación de las vulnerabilidades.
1.5	Se debe realizar auditoría de cumplimiento y revisión de la configuración de la plataforma.
1.6	Proporcionar la capacidad para desplegar una arquitectura por niveles (multi-tenant) basada en código ejecutada para todos los dispositivos a escanear.
1.7	Centralizar y automatizar la actualización de vulnerabilidades y amenazas diariamente.
1.8	Configurar los resultados por un periodo de tiempo después luego expirarán y serán purgados de la base de datos automáticamente.
1.9	Proporcionar control de acceso basado en roles y perfiles para controlar a los usuarios el acceso a la plataforma.
1.10	El acceso a la herramienta se debe hacer a través de credenciales.

1.11	Proporcionar exploración activa y de análisis de red pasiva para el descubrimiento de activos.
1.12	Proporcionar escaneo de aplicaciones web
1.13	Escanear anfitriones muertos (dispositivos que no responden a un ping)
1.14	Uso opcional del comando netstat para la enumeración rápida y precisa de los puertos abiertos en un sistema cuando se suministran credenciales.
1.15	Compatible con el uso de SMB y WMI para la digitalización de los sistemas Windows.
1.16	Iniciar automáticamente los servicios de registro remoto en los sistemas Windows cuando ejecuta un análisis con credenciales, luego automáticamente se detendrían los servicios de nuevo una vez finalizada la exploración.
1.17	Detectar nuevos dispositivos y enviar alertas y las notificaciones de correo electrónico, registro del sistema, o la consola.
1.18	Poner en marcha de forma automática el análisis de vulnerabilidades en nuevos dispositivos.
1.19	Proporcionar una cantidad significativa de comprobaciones de vulnerabilidad más allá del sistema operativo o plataforma Microsoft Windows.
1.20	Seguir los cambios de DHCP mediante la asociación de los resultados del análisis con los nombres de los hosts.
1.21	Preservar los resultados del análisis de los sistemas inactivos por un período personalizable y de identificación de las vulnerabilidades en el tiempo
1.22	Incluir salida detallada de los resultados de exploración para incluir información tal como versiones de librerías DLL o ejecutables esperados y los encontrados.
1.23	Informar sobre las debilidades conocidas en un objetivo dado, identificado por las organizaciones de asesoramiento de seguridad (por ejemplo, Vulnerabilidades y Exposiciones Comunes base de datos (CVE) o la base de datos de Open Source vulnerabilidad (OSVDB) o la Security Focus Bugtraq (BID) o cualquier combinación de ellos).
1.24	Proporcionar auditoría de parches para los sistemas operativos de Microsoft y aplicaciones, como Windows, Internet Explorer, Microsoft Office, IIS, Exchange, y otros más.
1.25	Proporcionar auditoría de parches para los principales sistemas operativos Unix a incluir Mac OS, Linux, Solaris, IBM AIX, HP-UX, y otros más.
1.26	Proporcionar revisión de parches para la infraestructura de red para incluir Cisco, Palo-Alto, Juniper, etc
1.27	Proporcionar una integración con los sistemas de administración de parches para la auditoría e informes de parches delta en los resultados de digitalización a incluir Microsoft WSUS / SCCM, Redhat Satellite, IBM Tivoli Endpoint Manager, Altiris, VMware Go.
1.28	Proporcionar una vista consolidada de todos los resultados de auditoría de vulnerabilidad y cumplimiento.
1.29	Proporcionar puntos de referencia de seguridad y auditoría de configuración para las mejores prácticas de proveedores o fabricantes como Microsoft, Cisco, PaloAlto y VMware.
1.30	Proporcionar verificación de los sistemas operativos de Microsoft para la configuración de seguridad y configuraciones.
1.31	Proporcionar la auditoría de los principales sistemas operativos Unix / Linux para la configuración de seguridad y configuración de aplicativos instalados.
1.32	Proporcionar auditoría de bases de datos para la configuración de seguridad y configuraciones.
1.33	Proporcionar auditoría de aplicaciones para la configuración de seguridad y configuración.
1.34	Proporcionar auditoría de infraestructura de red o equipos de comunicaciones, para su endurecimiento de seguridad y practicas recomendadas de configuración.
1.35	Facilitar la automatización completa de escaneo, informes y alertas.
1.36	Definir alertas basadas en el análisis de vulnerabilidades o los resultados de la auditoría de configuración.
1.37	Las acciones de alerta deben incluir: correo electrónico, creación y asignación de un ticket, inicio de un escaneo, generación de un evento syslog y generación automática de informes o reportes.

1.38	Proporcionar auditoría de parches para los sistemas operativos de Microsoft y aplicaciones, como Windows, Internet Explorer, Microsoft Office, IIS, Exchange, y otros más.
1.39	Proporcionar auditoría de parches para los principales sistemas operativos Unix a incluir Mac OS, Linux, Solaris, IBM AIX, HP-UX, y otros más.
1.40	Proporcionar revisión de parches para la infraestructura de red para incluir Cisco, Palo-Alto, Juniper y más.
1.41	Proporcionar una integración con los sistemas de administración de parches para la auditoría e informes de parches delta en los resultados de digitalización, a incluir Microsoft WSUS / SCCM, Redhat Satellite, IBM Tivoli Endpoint Manager, Altiris, VMware Go.
1.42	Realizar el seguimiento del ciclo de vida de las instancias de vulnerabilidad en que se refiere a los hosts individuales, así como el medio ambiente, para incluir cuando una vulnerabilidad fue descubierta, última vez observada, y mitigado o previamente-mitigado.
1.43	Proporcionar una vista consolidada de todos los resultados de auditoría de vulnerabilidad y cumplimiento.
1.44	Proporcionar puntos de referencia de seguridad y auditoría de configuración para las mejores prácticas de proveedores o fabricantes como Microsoft, Cisco, PaloAlto y VMware.
1.45	Proporcionar auditoría de VMWare ESXi y vCenter utilizando el SOAP API propio de VMware.
1.46	Proporcionar verificación de los sistemas operativos de Microsoft para la configuración de seguridad y configuraciones.
1.47	Proporcionar la auditoría de los principales sistemas operativos Unix / Linux para la configuración de seguridad y configuración de aplicativos instalados.
1.48	Proporcionar auditoría de bases de datos para la configuración de seguridad y configuraciones.
1.49	Proporcionar auditoría de aplicaciones para la configuración de seguridad y configuración.
1.50	Proporcionar auditoría de infraestructura de red o equipos de comunicaciones, para su endurecimiento de seguridad y practicas recomendadas de configuración.
1.51	Proporcionar auditoría de paquetes antivirus específicos por: instalación, ultimas actualizaciones y el estado de arranque del producto.
1.52	Proporcionar verificación de la información de identificación personal (PII) y otros contenidos sensibles o sensitivos.
1.53	Permitir que las plantillas utilizadas con políticas de auditoría puedan ser personalizables según las necesidades específicas de la organización. Donde se puedan definir controles internos para sistemas de TI.
1.54	Facilitar la automatización completa de escaneo, informes y alertas.
1.55	Proporcionar vistas separadas para vulnerabilidades activas, pasivamente descubiertas, asociadas a cumplimiento y riesgo en dispositivos móviles.
1.56	Proporcionar vistas de remediación que se priorizan y sean simplificadas para la audiencia de forma automática.
1.57	Proporcionar la capacidad de automáticamente agrupar objetivos, utilizando los resultados del análisis para generar listas de activos dinámicas.
1.58	Proporcionar funcionalidad de tickets de remediación integrada, que también puede enviar entradas a los sistemas de 3ª partes u otros fabricantes.
1.59	Compatible con la asignación de tickets a los usuarios individualmente.
1.60	Definir alertas basadas en el análisis de vulnerabilidades o los resultados de la auditoría de configuración.
1.61	Las acciones de alerta deben incluir: correo electrónico, creación y asignación de un ticket, inicio de un escaneo, generación de un evento syslog y generación automática de informes o reportes.
1.62	Debe ser compatible con la generación de informes o reportes personalizables
1.63	Proporcionar, en la capacidad de la presentación de informes, automatizar completamente para incluir la ejecución programada y la entrega de informe posterior a la exploración.

2	TIPO DE LICENCIAMIENTO
2.1	Un (1) año
2.2	Debe licenciarse para escanear dispositivos entre equipos de cómputo, servidores, equipos de red, hipervisores y dispositivos IoT como impresoras, cámaras, teléfonos IP, entre otros.
3	ACCESO A LAS BASES DE CONOCIMIENTO, VIDEOS Y DOCUMENTACIÓN TÉCNICA DEL PRODUCTO
3.1	Deberá entregar las claves y/o licencias para tal efecto, vía correo electrónico al Supervisor del Contrato o quien haga sus veces
4	ACTUALIZACIONES DEL PRODUCTO
4.1	El contratista será el encargado de realizar las actualizaciones y uso de la última versión estable, durante la vigencia del servicio de soporte técnico.

B	DESCRIPCION TECNICA DEL BIEN Y/O SERVICIO A ADQUIRIR
1	Suministro, instalación y configuración de una herramienta antivirus orientado a XDR para 400 endpoint

1	ESPECIFICACIONES DEL SOFTWARE ANTIVIRUS ENDPOINT A ADQUIRIR
1.1	Deberá haber participado en los 5 rounds de MITRE Engenuity
1.2	Deberá tener al menos el 100% de prevención, 100% de detección y 100% de coverage analítico según los resultados de las evaluaciones de MITRE Engenuity del round 5
1.3	Protección contra ataques de día 0 provenientes de Internet, incluidos los correos electrónicos y las páginas web maliciosas.
1.4	Debe detectar técnicas de explotación sin necesidad de utilizar firmas, patrones o heurísticas, enfocadas principalmente en la prevención de exploits lógicos, procesos vulnerables y exploits del sistema operativo, para sistemas Microsoft Windows.
1.5	Debe identificar distintas técnicas de explotación de vulnerabilidades, entre las que se encuentran Return Oriented Programming, Heap Spray, Jit Spray, Shell link, Structured Exception Handler, entre otros)
1.6	Debe proteger las aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box". Entre las aplicaciones predeterminadas se encuentran: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, varias versiones de Flash Player, Microsoft Silverlight entre otras.
1.7	Debe estar en la capacidad de crear un snapshot de forma automática de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar datos forenses sobre el evento.
1.8	Debe permitir la configuración perfiles de protección en modo de prevención o monitoreo.
1.9	Debe ejecutar la terminación del proceso en el cual fue identificado el intento de ejecución de una técnica de explotación siempre y cuando no sea un proceso crítico del sistema operativo.
1.10	Debe Prevenir técnicas de explotación que utilizan Dylib-Hijacking, ROP y JIT para Mac OS.
1.11	Debe prevenir técnicas de explotación que buscan secuestrar el flujo de control de un proceso mediante el monitoreo de intentos de enumeración de la distribución de la memoria para sistemas operativos Linux.
1.12	Debe prevenir la ejecución de técnicas de explotación que buscan redireccionar los flujos de entrada y salida estándares a sockets de red para sistemas operativos Linux.
1.13	Debe prevenir la ejecución de técnicas de explotación que utilizan return-oriented programming para sistemas operativos Linux.
1.14	Debe prevenir la ejecución del uso de ciertas áreas de memoria que son usualmente utilizadas para almacenar el payload de un ataque utilizando técnicas de heap spray, para sistemas operativos Linux.
1.15	Debe contar con políticas de prevención de técnicas de explotación, así como de compatibilidad, de manera predeterminada, con la finalidad de mejorar la experiencia del usuario final y reducir la creación de falsos positivos.

1.16	Debe estar en capacidad de proporcionar la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.
2	IDENTIFICACIÓN DE ATAQUES POST-EXPLOTACIÓN
2.1	Debe Identificar y prevenir de intentos de escalación de privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Mac y Linux
2.2	Debe detectar y terminar los comportamientos considerados como maliciosos mediante el análisis continuo de la cadena de eventos que sucedan en un endpoint. Esta detección debe considerar varios eventos y no sólo un evento para poder proporcionar un veredicto de la actividad maliciosa. La detección debe utilizar varias reglas preconfiguradas, las cuales deben de tener la capacidad de analizar varios eventos y no sólo un evento.
2.3	La protección de la solución no deberá depender de una conexión a la consola de administración.
3	PREVENCIÓN CONTRA MALWARE
3.1	Debe permitir la generación de hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas.
3.2	Debe enviar los ejecutables cuando su hash es desconocido para su análisis en un sandbox ubicado en la nube, con la finalidad de determinar si son maliciosos o benignos. Esta protección debe estar disponible para sistemas operativos Windows, Mac, Linux y Android.
3.3	Debe estar en capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.
3.4	Debe estar en capacidad de generar los hashes de archivos ejecutables que estén almacenados en la computadora con la finalidad de poder consultar su veredicto en una nube de inteligencia de amenazas. Lo anterior deberá de poder realizarse mediante un escaneo.
3.5	Debe estar en capacidad de enviar los archivos clasificados como maliciosos a cuarentena, ya sea que hayan sido identificados al momento de intentar ejecutarse o al momento de ser identificados mediante un escaneo.
3.6	Debe contar con un módulo de prevención con ransomware, el cual funciona a través de archivos de trampa que al intentar ser modificados genera una alerta y termina el proceso que está intentando llevar a cabo esas acciones.
3.7	Debe utiliza un modelo matemático generado a partir de aprendizaje de máquina para comparar una gran cantidad de características de un archivo ejecutable, de manera estática, para determinar si es malicioso. Esta protección debe estar disponible para sistemas operativos Windows y Mac.
3.8	Debe estar en la capacidad de identificar si la macro contenida en un documento de Word o Excel es maliciosa, sin necesidad de tener que ejecutar la macro ni observar su comportamiento o ejecución, para determinar si es maliciosa.
3.9	Debe estar en la capacidad de proporcionar protección contra malware sin necesidad de tener una conexión a la consola ni a Internet.
3.10	Debe estar en la capacidad de proporcionar protección contra malware sin necesidad de contar con firmas, patrones y/o heurísticas.
3.11	Debe permitir la configuración de políticas en modo de prevención o monitoreo.
3.12	Debe permitir poner los archivos detectados como maliciosos en una cuarentena, ya sea de manera automática o bajo demanda.
3.13	Al momento de realizar el escaneo, el consumo de recursos debe de ser mínimo y no debe impactar en la experiencia del usuario
4	ESCANEOS DE ARCHIVOS EJECUTABLES
4.1	Debe permitir realizar el escaneo de archivos ejecutables sin la necesidad de firmas.
4.2	Debe permitir programar el escaneo de archivos de manera semanal o mensual.
4.3	Debe permitir definir el día y la hora en la cual se iniciará el escaneo.
4.4	Al momento de realizar el escaneo, el consumo de recursos debe de ser mínimo y no debe impactar en la experiencia del usuario
4.5	Debe permitir habilitar el escaneo de dispositivos de almacenamiento removible.
4.6	Debe permitir crear listas blancas de carpetas para que sean excluidas del proceso de escaneo.

4.7	Debe permitir poner en cuarentena los archivos identificados como maliciosos, si es que la política está configurada de esta manera.
5	PROTECCIÓN CONTRA EL ROBO DE CONTRASEÑAS
5.1	Debe proporcionar una protección en memoria contra el uso de la herramienta de extracción de contraseñas Mimikatz o similares
6	RESTRICCIONES DE EJECUCIÓN
6.1	Debe restringir la ejecución de archivos a partir de directorios específicos alojados en los dispositivos.
6.2	Debe restringir la ejecución de archivos a partir de recursos compartidos.
6.3	Debe restringir la ejecución de archivos a partir de dispositivos USB o CD/DVD.
6.4	Debe restringir de manera granular la ejecución de procesos hijo definiendo el proceso padre y los procesos hijo a restringir o permitir.
6.6	Debe restringir granularmente la ejecución de procesos hijo sin necesidad de contar con una conexión a la consola de administración.
6.7	Debe contar con políticas de restricción de creación de procesos hijo configuradas de manera predeterminada.
6.8	Debe permitir crear excepciones para permitir la ejecución de archivos a partir de ciertas carpetas.
6.9	Debe estar en capacidad de crear excepciones para permitir la creación de procesos hijo.
6.10	Debe estar en la capacidad de crear excepciones para permitir la ejecución de archivos a partir de carpetas dentro de los dispositivos de almacenamiento removibles.
6.11	Debe permitir la configuración perfiles en modo de prevención o monitoreo
7	RESTRICCIÓN DE USO DE PUERTOS USB.
7.1	Debe de permitir generar perfiles que gestionen las siguientes características de bloqueo de puertos USB cuando se conecten los siguientes tipos de dispositivos: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB, adaptadores de red en formato USB.
7.2	Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo (discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB), tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada), y número de serie. Los parámetros tipo de dispositivo, tipo de permiso y fabricante deben de ser mandatorios.
7.3	Debe permitir la creación de políticas que utilicen los perfiles de bloqueo y de excepciones generados y sin ser excluyentes.
7.4	Debe permitir que las políticas generadas puedan asignarse a una computadora en particular o a un grupo de computadoras definido previamente.
7.5	Debe permitir la creación de excepciones permanentes utilizando los siguientes parámetros: tipo de dispositivo (discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles con conexión USB, unidades lectoras de discos floppy externas con conexión USB), tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada), y número de serie. Los parámetros tipo de dispositivo, tipo de permiso y

	fabricante deben de ser mandatorios. Estas excepciones permanentes no deben de depender de ser aplicadas a una política para que surtan efecto.
7.6	Debe de mostrar las violaciones a las políticas que se hayan registrado mostrando lo siguiente: horario, computadora, usuario, dirección IP, tipo de dispositivo, producto, fabricante y número de serie del dispositivo que intentó conectarse.
7.7	Deberá de soportada sistemas operativos Windows y Mac.
7.8	Debe permitir gestionar los puertos USB que permitan conectar dispositivos como: discos duros, unidades lectoras de CD-ROM externas con conexión USB, dispositivos de almacenamiento removibles portátiles, unidades lectoras de discos floppy externas con conexión USB.
7.9	Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo, tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada) y número de serie.
7.10	Deberá ser capaz de integrarse a Active Directory para establecer políticas de control de USB en base a grupos de LDAP.
7.11	Debe de permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable.
7.12	Debe estar en capacidad de añadir nuevos tipos de dispositivos agregando el GUID de Windows correspondiente.
8	FIREWALL DE HOST
8.1	Esta funcionalidad deberá de estar disponible para los sistemas operativos Windows y Mac.
8.2	Las siguientes funcionalidades deberán estar disponibles para sistemas operativos Windows: Se deberá controlar todas las comunicaciones entrantes y salientes utilizando direcciones IP.
8.3	Las reglas serán aplicadas de acuerdo con la ubicación del dispositivo dentro de la red interna de la entidad.
8.4	Debe de poder determinar, mediante la configuración, si el dispositivo se encuentra dentro o fuera de la organización.
8.5	La regla podrá especificar direcciones locales o remotas, así como puertos locales o remotos. También se podrá especificar el protocolo dentro de estas cuatro opciones: ICMP, TCP, UDP, ICMPv6.
8.6	Permitir habilitar el firewall nativo del sistema operativo.
8.7	Permitir o bloquear las comunicaciones de red entrantes.
8.8	Habilitar el modo stealth
8.9	Crear exclusiones por aplicación para permitir o bloquear programas de manera específica, utilizando la funcionalidad del sistema operativo conocido como BlundleID, estas deben ser concertadas desde el inicio de la ejecución del contrato con el supervisor.
9	VISIBILIDAD DE ENDPOINT
9.1	Deberá estar en la capacidad de generar un inventario de las aplicaciones instaladas en las computadoras con sistema operativo Windows, MacOS, Linux, etc.
9.2	Deberá estar en la capacidad de generar un inventario de características de hardware del endpoint, como mínimo cantidad de memoria RAM; tipo, marca y capacidad de procesador; almacenamiento del disco duro; identificar si es servidor, desktop o laptop; sistema operativo y arquitectura.
9.3	Deberá poder listar los usuarios locales creados en el endpoint y su respectivo estado (activo o inactivo)

9.4	Deberá poder listar los autoruns, servicios y unidades o carpetas compartidas para el caso de Windows.
9.5	Deberá mostrar los daemons para el caso de MacOS y Linux
9.6	Deberá mostrar las vulnerabilidades de los endpoints, ofreciendo detalles de los CVEs, incluyendo el nivel de severidad y métricas según la base de datos de vulnerabilidades de NIST
9.7	Deberá ser capaz de guardar un histórico diario de estos inventarios, para poder comparar cambios que hubiesen ocurrido. Este histórico deberá estar disponible por al menos 30 días.
9.8	La plataforma podrá contar con la capacidad de eliminar los IOC's de todos los dispositivos que tengan un agente instalado y siempre que tengan una ruta o hash, md5 respectivamente
10	ANÁLISIS DE ALERTAS E INVESTIGACIÓN DE ACTIVIDAD SOSPECHOSA
10.1	El producto deberá permitir la creación de una secuencia gráfica que correlacione las alertas individuales con el objetivo de describir la secuencia de un ataque.
10.2	El producto deberá de permitir hacer zoom in o zoom out para poder observar con mayor facilidad la secuencia mencionada anteriormente.
10.3	El producto deberá mostrar una advertencia cuando un ejecutable en particular, que forme parte de la secuencia gráfica, tenga un comportamiento sospechoso.
10.4	El producto deberá de mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, entidad que firmó el proceso, valor MD5 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox, valor SHA256 y línea de comandos de la ejecución.
10.5	El producto deberá de mostrar la actividad de cada proceso identificado, en columnas por categorías. Entre las categorías a incluir debe de estar la actividad de red, actividad de los archivos, actividad del registro, módulos ejecutados e intentos de inyección a procesos.
10.6	Para cada una de las actividades mencionadas anteriormente el producto deberá de desplegar los siguientes datos en columnas: fecha, nombre de la computadora, IP del host que generó la alerta, nombre de usuario, sistema operativo del host, tipo de actividad identificada, descripción de la actividad identificada, nombre del archivo asociado, nombre previo del archivo, ruta del archivo, ruta anterior del archivo, valor MD5 del archivo, valor SHA256 del archivo, ruta del archivo que fue el ejecutor del archivo, comando que utilizó el ejecutor del archivo, identificador del proceso que fue el ejecutor del archivo, valor MD5 del ejecutor del archivo que fue la causa raíz de la alerta, valor SHA256 del ejecutor del archivo que fue la causa raíz de la alerta, indicador sobre si el ejecutor de la alerta está firmado, entidad que firma el archivo que fue la causa raíz de la alerta, ruta del archivo que fue la causa raíz de la alerta, comando del archivo que fue la causa raíz de la alerta, valor SHA 256 del archivo que fue la causa raíz de la alerta, indicador sobre si el archivo que fue la causa raíz de la alerta está firmado, entidad que firma el archivo que fue la causa raíz de la alerta
11	VISUALIZACION
11.1	Deberá de contar con un dashboard en nube que permite visualizar alertas generadas de distintas fuentes.
11.2	Deberá correlacionar alertas de datos de los agentes instalados en los endpoint y agruparlas dentro de incidentes
11.3	Deberá de poder mostrar el número total de alertas e incidentes, y debe incluir la capacidad de filtrar la información de forma flexible

11.4	El producto deberá permitir la creación de una secuencia gráfica que correlacione las alertas individuales con el objetivo de describir la secuencia de un ataque.
11.5	El producto deberá de mostrar información específica de cada proceso involucrado en la secuencia gráfica.
11.6	En la pantalla emergente, en caso de estar disponible, deberá de mostrarse los datos relacionado con el perfil de comportamiento y la ejecución del archivo.
11.7	El producto deberá mostrar una advertencia cuando un ejecutable en particular, que forme parte de la secuencia gráfica, tenga un comportamiento sospechoso.
11.8	El producto deberá de mostrar datos generales de la ejecución de un proceso que forme parte de la secuencia gráfica, entre los que se encuentran ruta de ejecución, nombre de usuario que ejecutó el proceso, tiempo de su ejecución, entidad que firmó el proceso, valor MD5 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox, valor SHA256 y línea de comandos de la ejecución.
11.9	El producto deberá mostrar la actividad de cada proceso identificado, en columnas por categorías. Entre las categorías a incluir debe de estar la actividad de red, actividad de los archivos, actividad del registro, módulos ejecutados e intentos de inyección a procesos.
11.10	El producto deberá utilizar el aprendizaje automático supervisado y no supervisado para establecer líneas de base del comportamiento habitual del usuario y del dispositivo y detectar desviaciones de comportamiento que caracterizan la actividad anómala.
11.11	El producto deberá de proporcionar la capacidad de decodificar cadenas de caracteres codificadas en base-64 para mostrarlo en texto plano.
11.12	El producto deberá de poder identificar, de todas las actividades mencionadas anteriormente, aquellas que sean maliciosas o altamente sospechosas y separarlas en una categoría de fácil acceso para el analista.
11.13	Inteligencia de amenazas compartida para distribuir inteligencia de amenazas de crowdsourcing del servicio de análisis de malware basado en la nube a firewalls, agentes de punto final y servicios de detección y respuesta
11.14	Para cada una de las actividades mencionadas anteriormente el producto deberá de desplegar los siguientes datos en columnas: fecha, nombre de la computadora, IP del host que generó la alerta, nombre de usuario, sistema operativo del host, tipo de actividad identificada, descripción de la actividad identificada, nombre del archivo asociado, nombre previo del archivo, ruta del archivo, ruta anterior del archivo, valor MD5 del archivo, valor SHA256 del archivo, ruta del archivo que fue el ejecutor del archivo, comando que utilizó el ejecutor del archivo, identificador del proceso que fue el ejecutor del archivo, valor MD5 del ejecutor del archivo que fue la causa raíz de la alerta, valor SHA256 del ejecutor del archivo que fue la causa raíz de la alerta, indicador sobre si el ejecutor de la alerta está firmado, entidad que firma el archivo que fue la causa raíz de la alerta, ruta del archivo que fue la causa raíz de la alerta, comando del archivo que fue la causa raíz de la alerta, valor SHA 256 del archivo que fue la causa raíz de la alerta, indicador sobre si el archivo que fue la causa raíz de la alerta está firmado, entidad que firma el archivo que fue la causa raíz de la alerta.
11.15	El producto deberá mostrar si existió una inyección de código o si el protocolo RPC es utilizado en otro proceso desde una computadora local o remota.
11.16	El producto deberá proporcionar de manera gráfica la interacción que existe con las direcciones IP que se quieran investigar. Deberá de poder mostrar diferentes opciones de vistas como la ubicación geográfica o los archivos ejecutables que generaron esa comunicación.

11.17	El producto deberá proporcionar de manera gráfica la interacción que existe entre uno o varios procesos que sean investigados. La gráfica deberá de mostrar la interacción entre los procesos, y si existe una relación entre las computadoras que ejecutan dichos procesos, entre otros aspectos.
12	CONFIGURACIÓN Y ELEMENTOS DE IDENTIFICACIÓN
12.1	El producto deberá de contar con mecanismos de generación de alertas considerando el comportamiento mostrado por los procesos de las computadoras.
12.2	Las alertas generadas por el comportamiento de los procesos no deberán de utilizar firmas o heurísticas.
12.3	Cada alerta generada por el comportamiento de los procesos deberá de tener una descripción del comportamiento identificado.
12.4	Cada alerta generada deberá de contar con una clasificación de acuerdo a su severidad.
12.5	El producto deberá permitir al analista definir comportamientos de procesos para que generen alertas.
12.6	El producto deberá de permitir la generación de excepciones a los comportamientos de los procesos que hayan sido identificados como maliciosos o sospechosos.
12.7	El producto deberá de permitir deshabilitar, modificar, exportar o eliminar los comportamientos que generen las alertas por el comportamiento de los procesos.
12.8	El producto deberá de soportar el uso de indicadores de compromiso tradicionales, incluyendo rutas de archivos, nombres de archivos, dominios, direcciones IP y hashes.
12.9	El producto deberá de permitir deshabilitar, modificar, exportar o eliminar un indicador de compromiso mediante un menú contextual.
12.10	El producto deberá de permitir la gestión de los indicadores de compromiso por comportamiento de procesos e indicadores de compromiso tradicionales mediante la consola de administración.
13	CARACTERÍSTICAS DEL AGENTE
13.1	El agente a instalar en los dispositivos deberá tener las siguientes características mínimas:
13.2	Soporte para las siguientes versiones de sistemas operativos: Windows 7 (32-bit, 64-bit, RTM & SP1; excepto Home), Windows Embedded 7 (Standard & POSReady), Windows 8.1 (32-bit, 64-bit; FIPS mode), Windows Embedded 8.1 Pro, Windows 10 Pro (32-bit and 64-bit), Windows 10 Enterprise LTSB, Windows 10 Education, Windows 10 Update 1809, Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter.
13.3	OSX 10.10 (Yosemite), OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14.
13.4	CentOS 6, CentOS 7, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16
13.5	Soporte para los siguientes ambientes virtuales: VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V
14	CONSOLA DE ADMINISTRACION
14.1	La consola de administración, debe ser el único punto de administración y control de todos los productos de la solución
14.2	La consola de administración debe permitir realizar, implementar y gestionar políticas de prevención de amenazas y mitigación de incidentes

14.3	Actualización y administración centralizada de la solución propuesta, permitiendo monitorear el estado de protección de los equipos y actualizarlos de forma centralizada y programada con actualizaciones incrementales
14.4	Controles frente al usuario
14.5	Defensa dedicada contra el Ransomware (Posibilidad de copiar archivos con posibilidad de restauración si se presenta un ataque)
14.6	Eliminación segura de archivos de cuarentena
14.7	Factor de doble autenticación para inicio de sesión de la consola
14.8	Navegación segura
14.9	Facilidad de uso
14.10	La consola de administración debe permitir realizar escaneo simultáneos, programados o manuales a todos los equipos de la red (por grupos o de manera individual)
14.11	La consola de administración debe informar mediante reportes los virus o amenazas que fueron detectadas, identificar los archivos y equipos de cómputo donde se presentó el evento
14.12	La consola de administración debe informar el estado actual de los equipos administrado
14.13	La consola de administración debe estar disponible en idioma español. De no estar disponible en idioma español se deberá entregar en idioma inglés
14.14	Análisis de riesgos en los endpoints identificar y reparar riesgos de la red y del sistema operativo a nivel de endpoints mediante tareas que puedan configurarse en la política para que se ejecuten recurrentemente en los endpoints objetivos
14.15	Sandbox proporcionar capa de protección contra amenazas avanzadas que realizan un análisis manual o automático y en profundidad de los archivos sospechosos
14.16	Inspector de proceso
14.17	Anti-phishing y filtrado de seguridad web
14.18	Control y refuerzo en los EndPoint (Cortafuego, control de dispositivos y control de contenido)
14.19	Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.
14.20	Cuenta con integración con Active Directory para la gestión de computadoras y configuración de políticas.
14.21	Cuenta con la capacidad de poder crear perfiles granulares.
14.22	Cuenta con la capacidad de poder crear políticas basadas en los perfiles creados.
14.23	Cuenta con la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizacionales de Active Directory.
14.24	Cuenta con la capacidad de crear grupos virtuales que pueden alimentarse de forma estática y dinámica.
14.25	La alimentación dinámica de los grupos virtuales podrá ser de forma estática y dinámica, siendo posible configurar para la forma dinámica el nombre de la computadora y dirección IP como mínimo.
14.26	Cada evento de prevención o notificación cuenta con información básica como tipo de evento, módulo que realizó la prevención, detalles de ese módulo, nombre de la computadora, nombre del usuario, sistema operativo, versión del agente, proceso que generó el evento de prevención, ruta de ejecución del proceso que generó el evento de prevención (en caso de estar disponible), horario y fecha del evento, información forense (en caso de estar disponible).
14.27	La consola deberá de ser proporcionada bajo un esquema software as a service.
14.28	Cuenta con un dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo a su criticidad en alta, media y baja), un resumen sobre los

	incidentes de seguridad, la cantidad de endpoints que tienen instalado el agente (clasificados por su plataforma), la cantidad de licencias disponibles y la versión del agente.
14.29	Cuenta con un dashboard donde se describen las características de los incidentes de seguridad que se han generado. Este dashboard debe de permitir analizar a mayor detalle las alertas de seguridad, incluyendo los reportes generados por el agente.
14.30	Integración con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas, a través de un API.
14.31	Debe permitir gestionar las excepciones en una pantalla específica.
14.32	Debe permitir crear excepciones a reglas, mecanismos de detección y/o mecanismos de protección desde la consola. Estas excepciones deben de poder aplicarse a una computadora en específico, o a un grupo de computado
14.33	Deberá de poder utilizar los datos capturados por el agente que se utiliza para realizar las tareas de detección e investigación, sin necesidad de utilizar un segundo agente.
14.34	Deberá de contar con un dashboard que permite visualizar alertas generadas de distintas fuentes
14.35	Las columnas del dashboard deberán de ser configurables, para poder seleccionar las que sean del interés del analista.
14.36	El ancho de las columnas deberá de poder ser configurable.
14.37	La anchura de los renglones de las alertas deberá ser personalizables.
14.38	Las alertas deberán de poder ser filtradas utilizando los siguientes parámetros: ID de la alerta, Timestamp, Nombre del host, IP del host, Nombre de usuario, Severidad, Fuente de la alerta, Si la alerta constituye una detección o un bloqueo, Categoría, Nombre de la alerta, Descripción, Proceso que lo inició, Línea de comando del proceso que lo inició, Firma del proceso que lo inició, Nombre de la entidad que firmó el proceso, Tipo de evento, Nombre del proceso que generó la alerta, Comando del proceso que generó la alerta, Firma del proceso que generó la alerta, Nombre de la entidad que firmó el proceso que generó la alerta, Identificador de la alerta, IP del host, Tipo de evento, CID, Ruta del archivo, Valor MD5 del archivo, Valor SHA256 del archivo, Valor del registro, Llave completa del registro, IP local, Puerto local, Host remoto.
15	PLATAFORMA DE SANDBOXING
15.1	El agente deberá ser capaz de enviar automáticamente el archivo a un entorno de sandbox para ser emulado.
15.2	El sandbox deberá estar basado en nube y debe tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
15.3	El sandbox deberá soportar el análisis de 100 mil archivos por día. El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso.
15.4	Deberá garantizar la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que cuente como mínimo con las certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001.
15.5	Capacidad de realizar análisis de sandboxing en sistemas Windows, MacOS, Linux.
16	TELEMETRIA Y COLECCION DE EVENTOS
16.1	El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows:
16.2	Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.
16.3	Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
16.4	Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.

16.5	Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
16.6	Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto).
16.7	Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), resolución de dominio (hostname), tráfico entrante y saliente, país destino de la IP pública.
16.8	Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP.
16.9	Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardar llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado. Nombre del valor o llave modificado. Datos del valor modificado.
16.10	Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.
16.11	Logs de eventos de Windows.
16.12	El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos MacOS:
16.13	Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
16.14	Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
16.15	Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
16.16	Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
16.17	Logs de eventos de autenticación
16.18	El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Linux:
16.19	Para los archivos: las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Información del copiado o renombrado de los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos.
16.20	Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
16.21	Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
16.22	Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.

16.23	Logs de eventos de autenticación.
16.24	Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea.
16.25	Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.
16.26	Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando un endpoint en particular genere ese comportamiento.
16.27	Deberá de contar con un dashboard que permita visualizar alertas generadas de distintas fuentes.
16.28	El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración.
16.29	Deberá de contar con un dashboard que permita visualizar alertas generadas de distintas fuentes.
16.30	El timeline del ataque deberá mostrar el intento de ataque en diferentes fases de explotación acorde al Framework MITRE ATT&CK, tales como Ejecución, Persistencia, Descubrimiento, Desplazamiento Lateral, Command & Control, Exfiltración.
17	GESTION DE INCIDENTES
17.1	Deberá agrupar todas las alertas relacionadas a un incidente de seguridad de manera automática.
17.2	Por cada incidente mostrado deberá mostrar los elementos relacionados como ejecutables, hashes, direcciones IP.
17.3	Deberá mostrar los hosts y usuarios asociados al incidente.
17.4	Deberá ser posible asignar la revisión del incidente a un investigador con acceso a la consola, con el objetivo de llevar un orden sobre la atención de incidentes.
17.5	Capacidad de comentar los incidentes para detallar los avances realizados en la revisión.
17.6	Capacidad de clasificar el estado del incidente como abierto, en revisión, gestionado, cerrado, etc.
17.7	Capacidad de agrupar y desagrupar los incidentes de manera manual.
17.8	Capacidad de modificar la severidad del incidente de manera manual.
17.9	La consola deberá estar basada 100% en nube, con el objetivo de no depender ni administrar infraestructura física local. La nube del fabricante deberá contar con las siguientes características:
17.10	Contar con la certificación SOC2 Tipo II de AICPA, ISO 27001.
17.11	Contar con doble factor de autenticación para el login.
17.12	Permitir el acceso solo desde un rango de IP pública de la Entidad.
17.13	La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados.
17.14	Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.
17.15	Cuenta con la capacidad de crear grupos que pueden alimentarse de forma estática y dinámica.
17.16	Capacidad de personalización del dashboard para mostrar los widgets según las necesidades de la Entidad.
17.17	Capacidad de almacenar una auditoría de eventos sobre las acciones realizadas en la consola

17.18	Deberá permitir el envío automático de alertas al correo electrónico cuando se identifica una actividad maliciosa. Podrán aplicarse filtros a dichas alertas para solo mostrar las de mayor relevancia.
17.19	Deberá permitir la generación de reportes a través de plantillas preconfiguradas y también permitir definir reportes personalizados.
17.20	Mantener un historial de los reportes que han sido generados para su posterior consulta.
17.21	Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos
18	THREAT INTELLIGENCE
18.1	Capacidad de alimentar la plataforma de Indicadores de Compromiso (IOC) de manera manual o automática vía API
18.2	Los IOC soportados deberán ser de tipo Hash, Ruta, Nombre de archivo, Dominio, Dirección IP.
18.3	Capacidad de agregar IOC de manera individual o masiva (por ejemplo, subiendo un archivo CSV)
18.4	Capacidad de colocar un nivel de reputación, confiabilidad del IOC y una fecha de expiración.
18.5	Debe poder integrarse a una plataforma tercera de Threat Intelligence como Virus Total.
18.6	Mostrar un mapa geográfico que permita analizar la dirección IP detectada como parte de incidente, como mínimo deberá mostrar lo siguiente: fecha de registro, ISP (Internet Service Provider), país. La información deberá poder ser mostrada en base al país, proceso, puerto e IP destino.
18.7	Deberá contar con un dashboard que permita analizar el comportamiento del hash de un archivo en particular, mostrando su nivel de reputación y si dicho hash ha sido detectado en otras alertas e incidentes.
19	CAPACIDADES DE RESPUESTA
19.1	Deberá ser posible colocar en lista bloqueada y/o lista permitida uno o más hashes.
19.2	Deberá permitir colocar en cuarentena un archivo malicioso detectado y/o bloqueado. La colocación en cuarentena deberá poder realizarse de manera manual y automática.
19.3	Capacidad de extraer el archivo dump de la memoria RAM del endpoint a partir de una alerta revisada.
19.4	Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador
19.5	Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.
19.6	Capacidad de configurar reglas de automatización que permitan ejecutar una acción determinada en los endpoints en base condiciones de alertas de seguridad, como mínimo estas reglas deberán permitir las siguientes acciones de manera automática: aislar el endpoint, hacer un escaneo de malware, extraer el malware desde el endpoint.
19.7	Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones:
19.8	Listar procesos y archivos
19.9	Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux).
19.10	Ejecutar scripts basados en Python
19.11	Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes.

19.12	Deberá contar con una librería de scripts predefinidos y deberá ser posible configurar scripts personalizados basados en Python.
19.13	Capacidad de tareas remotas a múltiples endpoints, como mínimo cerrar procesos, eliminar archivos, eliminar y/o modificar claves de registro.
19.14	Mostrar sugerencias para las remediaciones de un equipo comprometido.
19.15	Capacidad de integración con un SIEM vía Syslog y plataformas SOAR para adquisiciones posteriores.
19.16	La plataforma deberá contar con una capa de automatización para realizar acciones de manera automática basada en filtros tanto generales como específicos en el que se incluyan, nombres, hostnames, IP's, alertas, severidad, etc.
20	TIPO DE LICENCIAMIENTO
20.1	Un (1) año
21	MEDIOS DE INSTALACION Y MANUALES
21.1	Medios físicos y/o acceso a los portales de descarga del fabricante
22	ACCESO A LAS BASES DE CONOCIMIENTO, VIDEOS Y DOCUMENTACIÓN TÉCNICA DEL PRODUCTO
22.1	Deberá entregar las claves y/o licencias para tal efecto, vía correo electrónico al supervisor del contrato o quien haga sus veces
23	ACTUALIZACION DEL PRODUCTO
23.1	El contratista será el encargado de realizar las actualizaciones y uso de la última versión estable, por el fabricante durante la vigencia del Licenciamiento adquirida en este contrato

C	TRANSFERENCIA DE CONOCIMIENTO
1	Capacitar a 2 funcionarios del grupo de TI para la administración de las consolas, instalación, configuración, pruebas y puesta en producción tanto del antivirus como tenable, con una duración de 20 horas, esta capacitación debe ser dictada por un experto de fábrica y fuera de las instalaciones de CREMIL.

D	SERVICIO DE SOPORTE TÉCNICO CON FABRICANTE Y LOCAL
1	El contratista debe ofrecer el soporte técnico durante un (1) año contado a partir de la fecha del acta de inicio y aprobación por parte del supervisor del contrato 7X24.
	El contratista deberá responder a los requerimientos o solicitudes realizados por CREMIL, en un esquema 7x24 con un tiempo de respuesta de 2 horas a partir de la solicitud, para soportar el primer nivel de atención a través de medios como el correo, línea telefónica, celulares, o mesa de ayuda por el personal asignado por el fabricante, asignando un número de caso para atender a la entidad.
3	Realizar una (1) visita anual en coordinación con el supervisor del contrato, para revisión y afinamiento de la instalación de la consola de administración del antivirus y de tenable.
4	El tiempo máximo para la atención y solución de un incidente o problema debe ser de cuatro (4) horas, contadas a partir del reporte de la novedad.
5	En el caso de actualización de versiones, el contratista deberá programar esta actualización con anterioridad y con aprobación del Supervisor del contrato, así mismo, deberá programar la

socialización de las funcionalidades de administración de las plataformas para los funcionarios que gestionen la solución.

EQUIPO DE TRABAJO:

PERFIL	FORMACIÓN	EXPERIENCIA PROFESIONAL
Un (1) Gerente de Proyecto	<p>Ingeniero de sistemas o electrónico o telecomunicaciones o afines conforme al núcleo básico SNIES</p> <p>Especialización o maestría en ingeniería conforme al núcleo básico SNIES</p> <p>Certificaciones en:</p> <p>PMP vigente o</p> <p>SCRUM MASTER</p>	Acreditar experiencia profesional con cinco (5) años en proyectos de seguridad informática ejecutados en contratos mediante la presentación de certificaciones cuyas actividades sean relacionadas con el objeto del presente proceso.
Un (1) Ingeniero implementador	<p>Ingeniero de sistemas o electrónico o telecomunicaciones o afines conforme al núcleo básico SNIES</p> <p>Especialización o maestría en: seguridad informática y/o Ciberseguridad.</p>	Acreditar experiencia profesional con cuatro (4) años en proyectos de SOC e implementación de plataformas de seguridad endpoint ejecutados en contratos mediante la presentación de certificaciones cuyas actividades sean relacionadas con el objeto del presente proceso.
Un (1) Ingeniero certificado de fabrica	Ingeniero de sistemas o electrónico o telecomunicaciones o afines conforme al núcleo básico SNIES.	Acreditar experiencia profesional con mínimo tres (3) años en contratos de seguridad informática.

CLÁUSULA QUINTA: - PLAZO DE EJECUCIÓN: El plazo de ejecución del objeto contractual será hasta el **30 DE NOVIEMBRE DE 2024**, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y suscripción del acta de inicio del Contrato. Será requisito de ejecución la aprobación de las garantías las cuales deberán ser publicadas por el contratista y aprobadas por la entidad a través de la plataforma SECOP II.

CLÁUSULA SEXTA: VALOR DEL CONTRATO: Para todos los efectos legales, fiscales y presupuestales el presente contrato es por la suma de **TRESCIENTOS CINCUENTA Y NUEVE MILLONES DE PESOS M/CTE (\$359.000.000,00) INCLUIDO IVA** (Según Aplique) e incluido impuestos, contribuciones y costos directos e indirectos a los que haya lugar, el cual se encuentra amparado con el Certificado de Disponibilidad Presupuestal No. 22724 de fecha 17 de junio de 2024, así mismo se detalla a continuación los valores unitarios ofertados por el contratista bajo la cual se realizará la respectiva facturación:

CUADRO ECONÓMICO:

ÍTEM	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	VR. UNITARIO ANTES DE IVA	VR. IVA	VR. UNITARIO INCLUIDO IVA	VR. TOTAL, INCLUIDO DE IVA
1	Renovación suscripción tenable.io para 1000 esstet (activos)	1.000	UNIDAD	\$ 118.000,00	\$ -	\$ 118.000,00	\$ 118.000.000,00
2	Suministro, instalación y configuración de una herramienta antivirus orientado a XDR endpoint	400	UNIDAD	\$ 411.764,71	\$ 78.235,29	\$ 490.000,00	\$ 196.000.000,00
3	Servicio de soporte técnico con fabricante y local 7x24 por un (1) año	1	ANUAL	\$ 37.815.126,05	\$ 7.184.873,95	\$ 45.000.000,00	\$ 45.000.000,00
TOTAL				\$ 38.344.890,76	\$ 7.263.109,24	\$ 45.608.000,00	\$ 359.000.000,00

PARÁGRAFO: Conforme a lo establecido en los estudios previos que dieron origen al presente contrato y al Estatuto Tributario para el ítem No. 01 no aplica el impuesto del IVA en ocasión a lo establecido en el artículo 476 Servicios excluidos del impuesto sobre las ventas. Nota 1. Se exceptúan del impuesto los siguientes servicios y los bienes relacionados explícitamente a continuación: (...) 20. Adquisición de licencias de software para el desarrollo comercial de contenidos digitales, de acuerdo con la reglamentación expedida por el Ministerio de Tecnologías de la Información y Comunicaciones. (...) Categoría 15 Software de control de versiones: Software que permite gestionar los diversos cambios que se realizan sobre los elementos de algún producto o una configuración del mismo; Para el ítem No. 02 el antivirus se descarga y se instala en el equipo, por lo tanto, no todo se maneja en la nube dando aplicabilidad al impuesto de IVA del 19%, finalmente para el ítem No. 03 Servicio de soporte. Aplica el impuesto de IVA del 19%.

DISTRIBUCIÓN DE LOS RUBROS PRESUPUESTALES:

CDP	RUBRO	DESCRIPCIÓN	RECURSO	FUENTE – SITUACIÓN	VALOR DEL CDP	VALOR DEL CONTRATO	REDUCCIÓN
CDP 22724	A-02-02-01-004-007	EQUIPO Y APARATOS DE RADIO, TELEVISIÓN Y COMUNICACIONES	20	CSF Propios	\$ 346.830.473,00	\$ 314.000.000,00	\$ 32.830.473,00
	A-02-02-02-008-003	SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS (EXCEPTO LOS DE SERVICIOS DE INVESTIGACION, URBANISMO, JURÍDICOS Y DE CONTABILIDAD)	20	CSF Propios	\$ 73.169.527,00	\$ 45.000.000,00	\$ 28.169.527,00
TOTALES					\$ 420.000.000,00	\$ 359.000.000,00	\$ 61.000.000,00

CLÁUSULA SÉPTIMA: - FORMA DE PAGO: La Caja de Retiro de las Fuerzas Militares pagará al contratista el valor del contrato, en un (01) pago total contra entrega total de los servicios contratados.

Para el pago se deberán presentar los siguientes documentos:

1. Presentación en debida forma de la factura y cargue de la misma en el SECOP II.
2. Acta de inicio suscrita por el supervisor del contrato y el contratista (Este documento se requiere para el primer pago).
3. Informe del supervisor donde se especifiquen las actividades adelantadas por el contratista.
4. Certificación expedida por el Representante Legal o por el Revisor Fiscal según sea el caso, del pago de sus obligaciones a los sistemas de Salud, Pensión, Riesgos Laborales y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje SENA, del último mes, junto con la copia de la planilla de pago.
5. En el evento que la persona jurídica tenga personal contratado mediante prestación de servicios, se deberá certificar que estos están cumpliendo con la obligación de pago a Seguridad Social integral.

La factura debe cumplir los requisitos establecidos en el artículo 617 del Estatuto Tributario. a) Estar denominado expresamente como factura de venta (Régimen simplificado o régimen común). b) Apellidos y nombre del adquirente de los bienes y/o servicios. c) Llevar un número que corresponda a un sistema de numeración consecutiva de facturas de venta. d) Fecha de expedición. e) Descripción específica o genérica de los bienes y/o servicios. f) Valor total de la operación. g) El nombre del impresor de la factura. h) Indicar la calidad de retenedor del impuesto sobre las ventas. i) Al momento de la expedición de la factura, los requisitos de los literales a), b), d) y h) deberán estar previamente impresos a través de los medios litográficos, tipográficos o técnicas industriales de carácter similar. Cuando el contribuyente utilice un sistema de facturación por computador o máquinas registradoras, con la impresión efectuada por tales medios se entienden cumplidos los requisitos de impresión previa. El sistema de facturación deberá numerar en forma consecutiva las facturas y se deberá proveer los medios necesarios para su verificación y auditoría. j) El contratista deberá verificar si conforme a la Resolución 042 de 2020 y modificaciones emitida por la Dirección de Impuestos y Aduanas Nacionales DIAN le es aplicable la presentación de facturación electrónica, así como también tener en cuenta los lineamientos establecidos por el Ministerio de Hacienda y Crédito Público conforme a las Circulares Externas Nos.16 del 09 de marzo de 2021 y 20 del 12 de abril de 2021 expedidas por la Administración del Sistema de Información Financiera de SIF NACIÓN, donde se reglamenta la interoperabilidad de la factura electrónica con fines de masificación y control fiscal, por lo que previamente deberá coordinar con el supervisor contractual el procedimiento fijado por CREMIL para el recibo, aceptación y trámite de la factura electrónica por parte de CREMIL.

Nota 1: Se entienden incluidos como parte del valor del contrato, todos los impuestos, derechos, tasas, gastos directos o indirectos y contribuciones que se generen con ocasión o como efecto del contrato, los cuales corren a cargo del Contratista.

Nota 2: El valor de la factura se emitirá en pesos colombianos, previa recepción de los bienes y/o servicios prestados y recibidos a satisfacción

Nota 3: La Caja de Retiro de las Fuerzas Militares CREMIL, realizará los pagos previa disponibilidad del PAC y liquidez de la Tesorería.

PARÁGRAFO PRIMERO: El valor del contrato será consignado en la **CUENTA CORRIENTE** No. **21004264377** del **BANCO CAJA SOCIAL** a nombre de **UNIÓN TEMPORAL CREMIL 2023**, identificado con **NIT. 901.783.613-2**, de acuerdo con la certificación bancaria remitida por el contratista por la plataforma SECOP II.

CLÁUSULA OCTAVA: - LUGAR DE PRESTACIÓN DEL SERVICIO Y/O ENTREGA DE LOS BIENES. De acuerdo con el objeto contractual, el lugar de ejecución se realizará por medios virtuales seguros, y cuando se

requiera de presencialidad se debe realizar en la sede de la Caja de Retiro de las Fuerzas Militares en la ciudad de Bogotá D.C., sede edificio BOCHICA Interior 2 ubicada en la Carrera 10 N°. 27 – 00, o en la sede que designen los supervisores.

CLÁUSULA NOVENA: - PRÓRROGA DE PLAZO: Cuando EL CONTRATISTA demuestre fuerza mayor o caso fortuito u otro eximente de responsabilidad contractual deberá realizar los mismos trámites previstos en la cláusula vigésima quinta, la modificación del contrato se hará con el lleno de los requisitos legales establecidos para tal efecto. **PARÁGRAFO PRIMERO:** Teniendo en cuenta el riesgo previsible de insumo previsto en la matriz de riesgos del proceso de selección, el cual se encuentra asignado al contratista, CREMIL no aprobará prorrogas al contrato por este concepto, ni adiciones por el alza en el valor del insumo. **PARÁGRAFO SEGUNDO:** Durante los plazos de prórroga que se concedan al CONTRATISTA, quedan vigentes todas las obligaciones establecidas en el presente documento, igualmente EL CONTRATISTA se obliga a prorrogar la vigencia de la garantía con las coberturas que así lo requieran por el tiempo estipulado.

CLÁUSULA DECIMA: - TERMINACIÓN, MODIFICACIÓN E INTERPRETACIÓN UNILATERAL DEL CONTRATO: LA CAJA puede terminar, modificar y/o interpretar unilateralmente el contrato, de acuerdo con los artículos 15 a 17 de la Ley 80 de 1993, cuando lo considere necesario para que el contratista cumpla con el objeto del presente Contrato.

CLÁUSULA DECIMA PRIMERA: CAUSALES DE TERMINACIÓN: Este contrato se dará por terminado en cualquiera de los siguientes eventos: a) Por mutuo acuerdo de las partes, siempre que con ello no se causen perjuicios a la entidad. B) Por agotamiento del objeto o vencimiento del plazo. C) Por alguna causal eximente de responsabilidad contractual debidamente comprobada y soportada jurídicamente d). Por incumplimiento parcial o total de las obligaciones pactadas entre las partes en el contrato. **PARÁGRAFO:** En caso de terminación anticipada por mutuo Acuerdo entre las partes, LA CAJA pagará al CONTRATISTA, los valores proporcionales al tiempo de servicios prestados, se dejará constancia de ello en documento suscrito por las partes.

CLÁUSULA DECIMA SEGUNDA LIQUIDACIÓN. – Teniendo en cuenta que el objeto contractual es de tracto sucesivo procede su liquidación de conformidad con los artículos 60 de la Ley 80 de 1993, y artículo 11 de la ley 1150 de 2007.

CLÁUSULA DECIMA TERCERA: DECLARACIÓN DE INHABILIDAD: El contratista manifiesta bajo la gravedad del juramento, que se entiende prestado con la firma de este documento, no encontrarse incurso en causal de inhabilidad, incompatibilidad o prohibición legal para celebrar y ejecutar el presente contrato. **PARÁGRAFO:** EL CONTRATISTA responderá por haber ocultado al contratar inhabilidades, incompatibilidades o prohibiciones o haber suministrado información falsa.

CLÁUSULA DECIMA CUARTA - GARANTÍAS: En cumplimiento a de los riesgos que deben cubrir las garantías en la contratación descritas en sus apartes i) y ii) del artículo 2.2.1.2.3.1.1 y artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015, y teniendo en cuenta el presente proceso, se considera que se constituyan pólizas a favor de la CAJA DE RETIRO DE LAS FUERZAS MILITARES – CREMIL con NIT No. 899.999.118 1, así:

Las pólizas no expirarán por falta de pago de la prima o revocatoria unilateral.

TIPO RIESGO	PÓLIZAS EXIGIBLES
CALIDAD DEL SERVICIO.	Por un valor equivalente al veinte por ciento (20%) del valor del contrato, por un término igual al plazo de ejecución del contrato y un (1) año más.
CUMPLIMIENTO DEL CONTRATO.	Por un valor equivalente al treinta por ciento (30%) del valor del contrato, por un término igual al plazo de ejecución del contrato y seis (6) meses más.

PARÁGRAFO 1: Las vigencias de todos los amparos deberán ajustarse a las fechas de suscripción del contrato, y de la terminación del plazo de ejecución del mismo, según sea el caso. El hecho de la constitución de estos amparos no exonera al CONTRATISTA de las responsabilidades legales en relación con los riesgos asegurados. Dentro de los términos estipulados en el contrato, ninguno de los amparos otorgados podrá ser cancelado o modificado sin la autorización expresa de la CAJA DE RETIRO DE LAS FUERZAS MILITARES.

PARÁGRAFO 2: El CONTRATISTA deberá mantener vigente las garantías, amparos y pólizas a que se refiere esta cláusula y serán de su cargo el pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, cada vez que se disminuya o agote por razón de las sanciones que se impongan.

Estos mecanismos de cobertura son requeridos por la CAJA DE RETIRO DE LAS FUERZAS MILITARES, teniendo en cuenta que el objeto de las mismas, sirven para respaldar el cumplimiento de todas y cada una de las obligaciones que surgen a cargo del contratista frente a la administración y/o terceros, por razón de la celebración, ejecución y liquidación del contrato.

PARÁGRAFO 3: Conforme con lo señalado en la Circular Conjunta 001 del 20 de agosto de 2021 de la Superintendencia Financiera de Colombia y la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, la garantía aportada por el proponente será objeto de la verificación y validación del origen y veracidad de la misma, ante la compañía de seguros o entidad financiera o bancaria que la emite y advertidas inconsistencias en relación a su autenticidad será causal de rechazo de la propuesta y sujeto a las consecuencias contractuales y judiciales a que haya lugar.

CLÁUSULA DECIMA QUINTA- EXCLUSIÓN DE LA RELACIÓN LABORAL: EL CONTRATISTA se obliga a utilizar personal idóneo para el desarrollo del objeto contractual, contratado por su cuenta y riesgo bajo su exclusiva responsabilidad, quedando obligado al pago de salarios, prestaciones sociales y al cumplimiento de todas las obligaciones laborales a que haya lugar de acuerdo con las normas legales y convencionales vigentes. En consecuencia, no existirá ningún tipo de vínculo laboral entre LA CAJA y el personal que utilice el CONTRATISTA para el cabal cumplimiento del objeto.

CLÁUSULA DECIMA SEXTA – INDEPENDENCIA DEL CONTRATISTA: EL CONTRATISTA es una entidad independiente de LA CAJA, y, en consecuencia, EL CONTRATISTA no es su representante, agente o mandatario. EL CONTRATISTA, no tiene la facultad de hacer declaraciones, representaciones o compromisos en nombre de LA CAJA, ni de tomar decisiones o iniciar acciones que generen obligaciones a su cargo.

CLÁUSULA DECIMA SÉPTIMA- AUSENCIA DE PRESTACIONES: Dada su naturaleza jurídica este contrato no constituye ni produce relación laboral alguna, por lo cual el CONTRATISTA no adquiere vínculo laboral alguno con La Caja y es el único responsable con la ejecución del objeto contratado. En consecuencia, no tendrá derecho a reconocimiento de ningún otro valor distinto al pago del determinado en la Cláusula Quinta – Valor del Contrato.

CLÁUSULA DECIMA OCTAVA: CONTROL Y VIGILANCIA: La vigilancia y control del cumplimiento de las obligaciones a cargo del CONTRATISTA serán ejercidas por el Coordinador del Grupo de Informática PD. ING. VICTOR AUGUSTO PATINO PENUELA o quien haga sus veces con el apoyo del OPS. ALFONSO FREDY DELGADO MILLAN, quienes verificarán la ejecución idónea y el cumplimiento del objeto del contrato, además quien acatará lo señalado en artículo 83 y 84 de la Ley 1474 de 2011. Las atribuciones de los supervisores serán las establecidas en la ley 1474 de 2011 en los artículos 83 y S.S., además los artículos 4.3.7, 4.4, 4.4.1, 4.4.2, 4.4.3, 4. 4. 4 y 6 del Manual de Contratación de la Entidad Estatal la "Guía para el ejercicio de las funciones de Supervisión e Interventoría de los Contratos del Estado" - G-EFSICE-01 de la Agencia Nacional de Compras Públicas y demás normas reglamentarias pertinentes al tema y entre otras las siguientes: • Colaborar con el contratista para la ejecución del contrato. • Exigir el cumplimiento de las obligaciones del contrato. • Atender y resolver las consultas relacionadas con el desarrollo del mismo. • Verificar aportes parafiscales y aportes al Régimen de Seguridad Social. • Solicitar la imposición de multas, informar el incumplimiento del contratista para hacer efectiva la Garantía Única y hacer exigible la cláusula penal pecuniaria o en último término solicitar la declaratoria de caducidad, cuando se configuren los requisitos para su declaratoria. • Liquidar el contrato de conformidad con lo dispuesto en el artículo 60 de la ley 80 de 1993 y el artículo 11 de la Ley 1150 de 2007, dentro de los cuatro meses siguientes al vencimiento del plazo pactado. • Los demás establecidos en el manual de contratación de la Entidad.

CLÁUSULA NOVENA - LIMITACIONES DEL SUPERVISOR: El Supervisor no estará facultado en ningún momento para adoptar decisiones que impliquen la modificación de los términos y condiciones previstas en el presente contrato, las cuales únicamente podrán ser adoptadas por los representantes legales de las partes, mediante la suscripción de una modificación al contrato principal.

CLÁUSULA VIGÉSIMA: PENAL PECUNIARIA: En caso de incumplimiento de cualquiera de las obligaciones emanadas del presente contrato, la CAJA podrá hacer efectiva a título de pena una suma equivalente al diez por ciento (10%) del valor del contrato, esta suma se considera como estimación anticipada de perjuicios que pueda sufrir la CAJA. PARAGRAFO: El valor del a penal será descontado de cualquier saldo que resultare de a favor del CONTRATISTA por razón de este contrato si lo hubiere se cobrará conforme al artículo 75 de la Ley 80 de 1993.

CLÁUSULA VIGÉSIMA PRIMERA: DEBIDO PROCESO: Durante la ejecución del contrato, LA CAJA podrá hacer uso de las acciones sancionatorias previstas en el presente contrato, las cuales se adelantarán respetando el derecho al Debido Proceso consagrado en el Artículo 29 de la Constitución Política y en cumplimiento del procedimiento regulado en el artículo 86 de la Ley 1474 de 2011. En todo caso, LA CAJA en el proceso sancionatorio que se adelante, brindará todas las garantías constitucionales y legales al CONTRATISTA para que ejercite su derecho a la defensa en audiencia y tenga la oportunidad de exponer las razones y/o motivos sobre los hechos generadores de la afectación de la ejecución contractual. En ningún caso procederá la imposición de sanción sin haberse brindado la oportunidad al CONTRATISTA de explicar las causas que impiden la ejecución normal y oportuna del contrato.

CLÁUSULA VIGÉSIMA SEGUNDA: SOBRE LAS MULTAS. En caso de mora o incumplimiento parcial de las obligaciones a cargo del Contratista, la CAJA impondrá multas sucesivas mediante Resolución motivada, cada una hasta por un monto equivalente al uno por ciento (1%) del valor del contrato y hasta el diez por ciento (10%) de su valor total, momento a partir del cual se considera afectada de manera grave y directa la ejecución del contrato. Las partes acuerdan descontar directamente del valor del Contrato o de la liquidación del mismo, si a ello hubiere lugar las sumas causadas por concepto de multas.

CLÁUSULA VIGÉSIMA TERCERA: EXIMENTES DE RESPONSABILIDAD CONTRACTUAL: EL CONTRATISTA no será responsable ni se considera que ha incurrido en incumplimiento de sus obligaciones por cualquier demora en la ejecución de cualquier servicio amparado por el mismo, si se presentare durante su

ejecución circunstancias de FUERZA MAYOR O CASO FORTUITO u otros hechos fuera de su control, conforme a las definiciones del artículo 1° de la ley 95 de 1890 tales como: Guerra civil, insurrecciones, huelgas, motines, incendios, inundaciones, explosiones, terremotos, serios accidentes, cualquier otro acto de gobierno, prelacones gubernamentales, imposibilidad de obtención de licencias, certificados, reglamentos y demás documentos de gobierno que afecten la ejecución objeto del presente contrato y que estuviese fuera de su control razonable, EL CONTRATISTA se obliga a notificar por escrito a la CAJA cualquiera de los hechos anteriormente mencionados que puedan causar una demora, así mismo informará por escrito a LA CAJA dicha circunstancia cada quince (15) días calendario, hasta por un término máximo de sesenta (60) días, vencido el cual, LA CAJA podrá dar por terminado el contrato por medio de un acta de terminación de contrato, la cual será comunicada al CONTRATISTA sin que haya lugar a sanción alguna para éste. Cuando las circunstancias de FUERZA MAYOR O CASO FORTUITO debidamente comprobadas, no excedieren de (60) días, se levantará un Acta suscrita por las partes, con el fin de prolongar el plazo de ejecución en forma tal que se reponga el tiempo durante el cual ha existido dichas causales. **PARÁGRAFO PRIMERO:** No se considera eximente de responsabilidad los riesgos previsibles asignados al contratista, en especial el insumo del material y el precio pactado del mismo. **PARÁGRAFO SEGUNDO:** Ninguna de las Partes deberá ser responsable por cualquier fallo o retraso en la ejecución de este Contrato resultante de causas que excedan de su control razonable, incluyendo eventos impredecibles como, por ejemplo: actos de la naturaleza, desastres naturales, casos fortuitos, guerras, conflictos armados, actos del gobierno u órdenes judiciales. Incendios (excluyendo aquellos causados por la naturaleza), huelgas y cierres patronales en la empresa del subcontratista, no constituirán un evento de fuerza mayor. La Parte afectada por tal evento deberá notificar prontamente a la otra Parte de la ocurrencia del mismo y sus efectos en su capacidad de ejecución de los trabajos, lo cual deberá hacer en un lapso máximo de 10 días hábiles luego de haber detectado el evento. La falta de notificación hará de la Parte afectada, la responsable por los daños o pérdidas, lo cual podría evitar con la sola notificación. La Parte que ha reclamado un evento de fuerza mayor deberá hacer su mayor esfuerzo por mitigar el efecto de cualquier evento de fuerza mayor. Luego del cese del evento de fuerza mayor, la Parte afectada deberá notificar inmediatamente a la otra Parte de tal hecho, y hacer uso de sus mayores esfuerzos para reanudar lo más pronto posible, el normal desempeño de sus obligaciones de acuerdo con este Contrato. En el caso de que una de las Partes falle en el cumplimiento de alguna de sus obligaciones por alguna de las razones anteriormente expuestas, durante un periodo de 90 días o más desde la ocurrencia del evento de fuerza mayor, la otra Parte bajo su propio albedrío podrá extender el periodo de entrega basándose en la duración del retraso o de forma inmediata terminar el presente Contrato. Las Partes quedarán exentas de toda responsabilidad u obligación, en caso de aplicar la inmediata terminación de este Contrato debido a la ocurrencia de un evento de fuerza mayor debidamente comprobada conforme a la teoría de imprevisión. **PARÁGRAFO TERCERO:** En este caso EL CONTRATISTA se obliga a prolongar la Vigencia de las garantías del contrato.

CLÁUSULA VIGÉSIMA CUARTA: RESPONSABILIDAD DEL CONTRATISTA: EL CONTRATISTA es responsable por el cumplimiento del objeto establecido en la cláusula primera del presente Contrato. Así mismo, será responsable por los daños que ocasionen sus empleados y/o los empleados de sus subcontratistas a LA CAJA, en la ejecución del objeto del presente Contrato.

CLÁUSULA VIGÉSIMA QUINTA: SUSPENSIÓN: Por circunstancias de fuerza mayor o caso fortuito, se podrá de común acuerdo entre las partes, suspender el presente contrato mediante la suscripción de un acta donde conste tal hecho, sin que para los efectos del plazo extintivo se compute el tiempo de la suspensión, ni se harán exigibles las contraprestaciones mutuas. Una vez vencido el término de la suspensión, el contrato se reanudará automáticamente.

CLÁUSULA VIGÉSIMA SEXTA: CESIÓN DE DERECHOS ECONÓMICOS Y PATRIMONIALES: En caso que el CONTRATISTA decida efectuar una cesión y/o pignoración de derechos económicos deberá solicitar su aceptación y notificación por parte de LA CAJA, para lo cual deberá anexar como mínimo los siguientes documentos: 1) Contrato de cesión y/o pignoración de derechos económicos del contrato objeto de la cesión,

firmado por el cesionario y el cedente donde se relacione en forma explícita, lo siguiente: a) Valor de la cesión. B) Especificar si la cesión obedece al contrato principal y/o contratos adicionales. C) Aceptación por parte del cesionario de los descuentos de ley cuando aplique. 2) Certificado de existencia y representación legal del cesionario y el cedente cuando se trate de persona jurídica y/o certificado de inscripción cuando se trate de persona natural expedido por la cámara de comercio del domicilio correspondiente. 3) Certificación Bancaria con número de cuenta y beneficiario donde se deben consignar los valores cedidos.

CLÁUSULA VIGÉSIMA SÉPTIMA: CADUCIDAD ADMINISTRATIVA: CREMIL podrá declarar la caducidad administrativa del presente contrato por cualquiera de las causales previstas en la Ley 80 de 1993, de acuerdo a los procedimientos señalados en esta misma normatividad. La declaratoria de caducidad tendrá como efecto inmediato la terminación y liquidación del presente contrato. En la resolución que la declare se hará efectiva la cláusula penal pecuniaria y prestará mérito ejecutivo contra el CONTRATISTA y las partes que hayan constituido la garantía en los términos del artículo 52 de la Ley 80 de 1993.

CLÁUSULA VIGÉSIMA OCTAVA: INDEMNIDAD: - EL CONTRATISTA, mantendrá indemne a la Caja de toda reclamación, demanda o acciones legales, que tengan como causa las acciones directas del contratista, subcontratista o sus proveedores, siempre y cuando sea demostrada su responsabilidad, y que con estos actos se hayan derivado daños, lesiones o perjuicios materiales, en la integridad personal o patrimonial de los mencionados terceros durante la ejecución del contrato. Se consideran hechos imputables al contratista las acciones de su personal, ascensores, subcontratistas o proveedores o proveedores, así como el personal de estos, que produzcan deficiencias o incumplimientos. En caso de demandas, reclamaciones o acciones legales contra EL CONTRATANTE y que sean de responsabilidad demostrada del CONTRATISTA, conforme con lo pactado en este contrato, este será notificado luego de recibir el reclamo, obligándose a mantener indemne a la entidad y a responder por dichas reclamaciones y los costos que ellas generen hasta un 10% del valor del contrato.

CLÁUSULA VIGÉSIMA NOVENA: AMBIENTAL: El contratista deberá tomar todas las medidas conducentes para evitar la contaminación ambiental durante sus operaciones, cumplirá con todas las leyes ambientales aplicables y los actos administrativos de la Entidad que para tal fin se expiden, así como se sujetará a las normas relativas al control de la contaminación ambiental establecidas en dichas leyes, en las licencias o en los actos administrativos.

CLÁUSULA TRIGÉSIMA- DECLARACIONES DEL CONTRATISTA: El Contratista hace las siguientes declaraciones: a) Conoce y acepta los documentos del proceso de SAMC 004-2024. B) Tuvo la oportunidad de solicitar aclaraciones y modificaciones a los documentos del proceso de selección c) Se encuentra debidamente facultado para suscribir el presente contrato. D) Que al momento de la celebración del presente contrato no se encuentra en ninguna causal de inhabilidad e incompatibilidad. E) Está a paz y salvo con sus obligaciones laborales y frente al sistema de seguridad social integral de sus empleados. F) El valor del contrato incluye todos los gastos, costos, derechos, impuestos, tasas y demás contribuciones relacionadas con el cumplimiento del objeto del presente contrato. **PARÁGRAFO:** Frente al literal d) de la presente cláusula, EL CONTRATISTA responderá por haber ocultado inhabilidades, incompatibilidades o prohibiciones o haber suministrado información falsa.

CLÁUSULA TRIGÉSIMA PRIMERA: SOLUCIÓN DE CONFLICTOS: Conforme al artículo 68 de la Ley 80 de 1993, las partes se comprometen a utilizar los mecanismos de solución previstos en la mencionada ley. Dentro de los cinco (5) días hábiles siguientes a la presentación del conflicto las partes se reunirán para solucionarlo, para lo cual la CAJA DE RETIRO DE LAS FUERZAS MILITARES fijará fecha, hora y lugar; si existe acuerdo levantarán acta donde conste lo acordado; si subsiste el conflicto, el mecanismo para solucionarlo será escogido dentro de los diez (10) días hábiles siguientes. Para dicha escogencia se tendrán en cuenta las características

y condiciones especiales de cada conflicto, a fin de evitar dilaciones injustificadas que afecten la ejecución del contrato.

CLÁUSULA TRIGÉSIMA SEGUNDA- PERFECCIONAMIENTO Y EJECUCIÓN: Este contrato se entiende perfeccionado con la firma de las partes, el registro presupuestal correspondiente y la aprobación de las garantías solicitadas en el presente contrato al CONTRATISTA.

CLÁUSULA TRIGÉSIMA TERCERA - ACUERDO DE CONFIDENCIALIDAD: Las Partes mantendrán la “información confidencial” de manera confidencial y no revelarán, usarán, intentarán revelar o usar la misma a terceras partes. Las Partes podrán revelar la información confidencial a sus empleados siempre y cuando la misma sea necesaria para llevar a cabo los servicios estipulados en este Contrato y se limitará a lo estrictamente necesario en función de la necesidad de la información. Las Partes se obligan a que sus empleados no divulguen o revelen la información confidencial a terceras partes de la información que conozcan de los afiliados.

PARÁGRAFO PRIMERO: Las Partes usarán la información confidencial solamente para el desarrollo y cumplimiento de las obligaciones de acuerdo con lo establecido en este Contrato. **PARÁGRAFO SEGUNDO:** Las Partes no tomarán o intentarán tomar ningún tipo de ventaja o beneficio, derecho o privilegio para sí mismo o para con cualquier tercero, que no hubiera tenido disponible si no fuera por el acceso que este tenga a la información confidencial debido a su condición de CONTRATISTA o CONTRATANTE. **PARÁGRAFO TERCERO:** Las Partes tratarán de forma estrictamente confidencial la existencia de este contrato y no la revelará a ninguna persona, y de igual forma tampoco el hecho de que se haya recibido cualquier tipo de Información Confidencial. **PARÁGRAFO CUARTO:** “Información Confidencial” significa cualquier información y datos de naturaleza confidencial, incluyendo pero no siendo limitativo, los derechos de propiedad intelectual, propiedad, desarrollo, información técnica, mercadeo, ventas, clientes, operaciones, servicio, costos, finanzas, know-how, negocios o procesos de información, técnicas de programación de computadoras, planos, muestras, dispositivos y pruebas, y todo el soporte de red registrado que contenga o revele dicha información o técnicas, y cualquier información personal, se encuentre está marcada o no con las palabras “confidencial” o “propiedad” o sus equivalentes. Las Partes y sus directores, jefes, empleados, agentes y consultores deberán mantener la Información Confidencial de la otra Parte en confidencia y debido resguardo, y deberá prevenir su divulgación o cualquier tipo de uso distinto a los establecidos en este Contrato sin el previo consentimiento de la Parte reveladora, excepto en los siguientes casos: a) Fue notificado a la Parte receptora antes de la divulgación de la misma por la Parte reveladora; b) Es o llegase a ser del conocimiento del público en general a través de Terceros ajenos a la Parte receptora; c) Es revelada a la Parte receptora a través de Terceros con buena fe, y no en violación de cualquier acuerdo de confidencialidad con la obligación de guardar secreto por parte de la Parte reveladora o alguno de sus asociados o filiales; d) Es desarrollada por la Parte receptora independientemente de alguna revelación realizada, como se evidencia de los registros de la Parte receptora; Es requerida su divulgación por la Ley o una Corte con jurisdicción competente, previendo sin embargo que la Parte receptora deberá notificar a la Parte reveladora razonablemente con antelación a la divulgación, de tal manera que las Partes puedan solicitar una orden de protección apropiada, o de lo contrario impugnar la divulgación.

CLÁUSULA TRIGÉSIMA CUARTA: PUBLICACIÓN: De conformidad con lo establecido en la Ley 1150 de 2007 los contratos estatales sólo se publicarán en el Sistema Electrónico para la Contratación Pública – SECOP II que administra la Agencia Nacional de Contratación Pública-Colombia Compra Eficiente.

CLÁUSULA TRIGÉSIMA QUINTA: DOMICILIO: Para todos los efectos legales y fiscales. Las partes acuerdan fijar como domicilio la ciudad de Bogotá D.C.

El presente documento se entiende aprobado con la firma electrónica de las partes y el respectivo cargue en la plataforma electrónica SECOP II.

Elaboró:



PS. DAYRIS ARGOTE BAYONA
Comité Jurídico Evaluador



PS LAURA JOHANA VILLA RODRÍGUEZ
Comité Económico Evaluador



PD. JAVIER MAURICIO ESPINOSA MANDUANO
Comité Técnico Evaluador

Revisó y Aprobó:



ING VICTOR AUGUSTO PATIÑO PEÑUELA
Coordinador Grupo de Informática
Coordinador del Proceso Contractual