ASPECTOS GENERALES

1.1 OBJETO

La **CAJA DE RETIRO DE LAS FUERZAS MILITARES CREMIL** pone a disposición de los interesados el documento de condiciones preliminares del proceso de invitación abierta que tiene por objeto:

CONTRATAR LA ADQUISICIÓN DE UN SOFTWARE ANTIVIRUS ORIENTADO A XDR (ENDPOINT) Y LA RENOVACIÓN DE LA SUSCRIPCION DE UNA HERRAMIENTA DE SEGURIDAD CON EL SERVICIO SOPORTE TECNICO DE FABRICA Y LOCAL PARA LA CAJA DE RETIRO DE LAS FUERZAS MILITARES.

1.2. ALCANCE DEL OBJETO

Las herramientas de seguridad tenable y XDR brindarán protección tanto a las aplicaciones, como PC´s, servidores y red de datos de la entidad de la siguiente manera:

- Proporcionarán la administración segura de la infraestructura de CREMIL.
- Proporcionarán la seguridad de la red de datos, sus servicios y el acceso a ellos a través de internet y dispositivos conectados internamente.
- Protección de puntos finales, servidores y dispositivos que acceden a datos de la entidad y los proteja de compromiso.
- Supervisarán de manera regular la exploración y el análisis de vulnerabilidades en la infraestructura y el acompañamiento en la remediación y soluciones temporales frente a los resultados de las vulnerabilidades detectadas.

1.2.1 Descripción general de los servicios:

- Renovar la suscripción de la herramienta de gestión de vulnerabilidadesTENABLE.IO (Vulnerability Management) para 1000 esset
- 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 esset (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 ESSET
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 platadorma.
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 período 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 Satelite, 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 auditoria de bases de datos para la configuración de seguridad y configuraciones.
1.33	Proporcionar auditoria de aplicaciones para la configuración de seguridad y configuración.
1.34	Proporcionar auditoria 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.
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 prevencion, 100% de deteccion y 100% de coverage analitico segun los resultados de las evaluaciones de MITRE Engeniuty del round 5
1.3	Protección contra ataques de día 0 provenientes de Internet, incluidos los correos electrónicos y las páginas web maliciosas.
14	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	**ESCANEO 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 sí 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 enpoint: 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.

2. Equipo de trabajo

A nivel de personal, el proponente debe garantizar el siguiente recurso humano, presentando las certificaciones laborales y/o contratos, las cuales podrán ser verificadas por Caja de Retiro de las Fuerzas Militares CREMIL.

PERFIL	FORMACIÓN	EXPERIENCIA PROFESIONAL
Un (1) Gerente de Proyecto	Ingeniero de sistemas o electrónico o telecomunicaciones o afines conforme al núcleo básico SNIES Especialización o maestría en ingeniería conforme al núcleo básico SNIES Certificaciones en: PMP vigente o SCRUM MASTER	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	Ingeniero de sistemas o electrónico o telecomunicaciones o afines conforme al núcleo básico SNIES Especialización o maestría en: seguridad informática y/o Ciberseguridad.	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.

Atentamente,

Coronel (R) VICTOR AUGUSTO PATIÑO PEÑUELA
Coordinadora Grupo Informática

Revisó:

PD CLAUDIA PATRICIA ROSERO HOYOS

Profesional de defensa TI