Radicado 0121007019802 /MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-43

Bogotá D.C., 13 Julio de 2021

Señor Subteniente
JESUS ENRIQUE RAMIREZ FLOR
Coordinador Grupo Sistema Integral de
Información -Tecnologías de la Información y las Comunicaciones (E) DIGSA
Avenida Calle 26 No.69-76 Centro Empresarial Elemento
Torre Tierra Piso 17
Bogotá D.C

Asunto: Evaluación técnica del proceso de contratación selección abreviada de menor cuantía No. 129-MDN-COGFM-JEMCO-DIGSA-2021.

Respetuosamente, me permito enviar al señor Capitán de Navío Subdirector Administrativo y financiero la evaluación técnica del proceso de selección abreviada de menor cuantía No. 129-MDN-COGFM-JEMCO-DIGSA-2021.cuyo objeto es "adquisición de una solución de protección de punto final que incluya EDR parchado de aplicaciones y seguridad para correo office 65 para la Dirección General de sanidad militar con el fin de continuar con el proceso.

EVALUACION ASPECTOS TECNICOS

ITEM	ADQUISICIÓN DE UNA SOLUCIÓN DE PROTECCIÓN DE PUNTO FINAL QUE INCLUYA EDR, PARCHADO DE APLICACIONES Y SEGURIDAD PARA CORREO OFFICE 365	SOFTICS INGENIEROS SAS
1.	**GENERALIDADES**	**Cumple**
1.1.	El oferente se compromete a no divulgar, trasmitir o compartir la información que reciba, conozca o genere de la Dirección General de Sanidad Militar durante y después del presente contrato. Por tanto, el oferente deberá firmar el Acuerdo de Confidencialidad para el Sector Defensa, el cual garantiza que la información suministrada y generada para el presente proceso será resguardada de acuerdo a la normatividad vigente y Directiva del CGFM 154-2014, la cual será socializada por el Supervisor dejando la respectiva acta. Este Acuerdo de Confidencialidad debe firmarse con el Acta de Inicio del contrato.	
1.2.	El personal del equipo de trabajo asignado al proyecto por parte del oferente y que deba realizar visita técnica a las instalaciones de DIGSA, debe cumplir con las normas de seguridad para el control, acceso y permanencia temporal en las instalaciones de la Dirección General de Sanidad Militar (documentación de identificación, carnetización y dotaciones de seguridad industrial si es el caso), razón por la cual, el oferente efectuará los trámites pertinentes y asumirá los costos a que haya lugar.	**Cumple**
1.3	El oferente (encargado contrato) y la DIGSA (supervisor del contrato), realizarán mínimo una (1) reunión de seguimiento mensual a la ejecución del contrato en las instalaciones de la Dirección General de Sanidad Militar, dejando el acta respectiva firmada por todos los asistentes.	**Cumple**

2.	**ADQUISICION DE UNA SOLUCION DE PROTECCION DE PUNTO FINAL QUE INCLUYA EDR y PARCHADO DE APLICACIONES**	**Cumple**
2.1.	**CARACTERÍSTICAS GENERALES DE LA PLATAFORMA DE PROTECCIÓN:**	**Cumple**
2.1.1	La solución deberá estar (aparecer), listada como una de las soluciones con la certificación de BEST PROTECTION 2019 según AV TEST, además deberá aparecer listada como una de las soluciones nombradas como PRODUCT OF THE YEAR 2019 según AV. Comparatives, así mismo debe estar listada como una de las soluciones recomendadas según NSS LABS de 2019 y como líder en forrester wave de cloud workload security.	**Cumple**
2.1.2	El oferente proveerá una plataforma de integral para protección de punto final, administración de parches y protección de correo Office 365 que admita una solución de seguridad de información modular capaz de proteger cualquier entorno empresarial en un método escalable y de alta disponibilidad para un mínimo de 450 dispositivos (servidores – computadores) y su implementación deberá ser por un período de 12 meses, contados a partir de la aprobación de la garantía única del contrato.	**Cumple**
2.1.3	El oferente deberá instalar desde ceros la consola de administración de la solución ofertada, y realizar las configuraciones, pruebas y ajustes que sean necesarios, para el correcto funcionamiento de toda la solución en todos los servidores y computadores de acuerdo a lo contratado.	**Cumple**
2.1.4	Durante la implementación y despliegue de la solución en todos los servidores y computadores de la DIGSA, el oferente deberá disponer de un técnico Profesional y/o especialista certificado en instalación y configuración o mediante soporte en sitio 3 días con disponibilidad del 100% para la DIGSA, así mismo de manera remota el tiempo necesario para terminar la configuración y puesta en marcha de la solución, para atender cualquier eventualidad en base a la instalación y puesta en marcha de la solución, incluyendo la atención requerida en productivo durante y después del montaje del servicio para verificar el funcionamiento de las plataformas.	**Cumple**
2.1.5	El oferente deberá efectuar una visita mensual de dos (2) horas mínimo presencial / virtual, durante la vigencia del licenciamiento/servicio para revisar el funcionamiento de la consola que administra la solución, verificar y resolver problemas que se encuentren registrados en dicha consola con respecto al control que ejerce el software antivirus y en general malware detectado, eliminado o en cuarentena, con el fin de efectuar potenciales ajustes a la parametrización del entorno, actualizaciones, que permita un control más efectivo de acuerdo con los casos que se van presentando; entregando un informe detallado al supervisor del contrato de las actividades realizadas y las recomendaciones referente a los últimos parches de seguridad y procedimientos, así como optimización de reglas y demás aspectos a tener en cuenta por los administradores de la solución en la DIGSA.	**Cumple**
2.2	**CONSOLA DE ADMINISTRACION:**	**Cumple**
2.2.1	El paquete de instalación debe entregarse como un solo dispositivo virtual (imagen virtual). Las plataformas de virtualización soportadas deben ser: a. VMware vSphere, VMware View, VMware Horizon suites b. Citrix XenServer, Citrix XenApp, Citrix XenDesktop c. Microsoft Hyper-V d. Red Hat Enterprise Virtualization e. Kernel-based Virtual Machine or KVM f. Oracle VM g. Nutanix	**Cumple**

2.2.2	El producto debe permitir la implementación centralizada de máquinas de escaneo dedicadas.	**Cumple**
2.2.3	Para fines de escalabilidad, el producto debe permitir que cualquier componente o servicio se instale de forma independiente o en un método agrupado.	**Cumple**
2.2.4	Para propósitos de escalabilidad, el producto debe tener componentes dedicados para servicios de base de datos, servicios de comunicación, actualización y servicios web.	**Cumple**
2.2.5	Para alta disponibilidad y balanceo de carga, el producto debe incluir un módulo dedicado de balanceador de carga disponible.	**Cumple**
2.3	**EL PRODUCTO DEBE OFRECER LAS SIGUIENTES CAPACIDADES (CARACTERÍSTICAS GENERALES)**	**Cumple**
2.3.1	La Licencia adquirida y la consola de administración deben ser únicas del titular de los derechos de autor del software en cuestión. Así mismo, ofrecer el correcto funcionamiento del software y rendimiento en donde se instalarán todos los servicios de seguridad (endpoint, EDR, Administración de parches, actualizaciones y seguridad perimetral para correo Microsoft de office 365), todo desde una única consola de administración debe manejarse como una solución integral de seguridad que no requiere la instalación de múltiples agentes.	**Cumple**
2.3.2	Todos los componentes se podrán actualizar con un solo click desde la consola de administración, sin depender de su orden de instalación ni de ningún otro requisito.	**Cumple**
2.3.3	Deberá permitir actualizaciones ha pedido que permitirán a los administradores elegir qué paquetes de servicios de seguridad se actualizarán para ahorrar ancho de banda.	**Cumple**
2.3.4	Debe usar una base de datos no relacional, sin requerir ninguna clave de licencia de terceros para implementaciones mayores que un cierto número de puntos finales.	**Cumple**
2.3.5	Las notificaciones deben mostrarse en el menú principal, con aspectos destacados de los elementos no leídos, con la capacidad de enviarlo por correo electrónico, alertando al administrador sobre problemas importantes: problemas de licencias, alertas de brotes de malware y / o máquinas desactualizadas.	**Cumple**
2.4	**PANEL DE CONSOLA DE ADMINISTRACIÓN PARA MONITOREO Y MANEJO DE INCIDENTES, EL PRODUCTO DEBE OFRECER:**	**Cumple**
2.4.1	Capacidad para agregar, eliminar, organizar, configurar y personalizar múltiples portlets de seguridad; así como soportar múltiples páginas.	**Cumple**
2.4.2	Capacidad para ofrecer información de seguridad en tiempo real con gráficos fáciles de leer.	**Cumple**
2.4.3	Capacidad para configurar el destino de los informes, el fondo del tipo de informe de seguridad, el intervalo de tiempo para la información portlet.	**Cumple**
2.5.	**CONSOLA DE ADMINISTRACIÓN DEL INVENTARIO DE RED. PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFRAESTRUCTURA, EL PRODUCTO DEBE OFRECER:**	**Cumple**
2.5.1	Integración con Microsoft Active Directory, VMware vCenter, Citrix Xen para importar el inventario e información de estas plataformas.	**Cumple**
2.5.2	Tiempo de sincronización configurable (en horas) con Microsoft Active Directory.	**Cumple**
2.5.3	Integración con Microsoft Hyper-V, RedHat Linux Virtual Machine, Oracle VM, KVM y cualquier otra máquina virtual que se descubra a través del descubrimiento de la red.	**Cumple**
2.5.4	Descubrimiento de redes para máquinas no integradas en Microsoft Active Directory, VMware vCenter, Citrix XenServer, tanto para estaciones de trabajo físicas como virtuales y servidores.	**Cumple**

2.5.5	Búsqueda en tiempo real, clasificación y filtrado por nombre, sistema operativo, dirección IP, FQDN o etiqueta.	**Cumple**
2.5.6	Capacidad de implementación remota y desinstalación del producto antimalware existente, capaz de cumplir con la función de desinstalación completa en los dispositivos con cualquier tipo de versión instalada anteriormente.	**Cumple**
2.5.7	Paquetes de instalación manual y configurable para el producto antimalware en el dispositivo que se requiera.	**Cumple**
2.5.8	Capacidad para configurar y ejecutar tareas de escaneo remoto.	**Cumple**
2.5.9	Capacidad para reiniciar remotamente un punto final.	**Cumple**
2.5.10	Capacidad para ver la sección de resultados de tareas centralizada con información detallada de cada subtarea.	**Cumple**
2.5.11	Capacidad para asignar políticas en todos los niveles de gestión.	**Cumple**
2.5.12	Capacidad para configurar la herencia de políticas y forzar la configuración de políticas.	**Cumple**
2.5.13	Capacidad para ver las propiedades detalladas de los puntos finales administrados, como el nombre, IP, sistema operativo, grupo, política asignada, el estado más reciente del malware, los últimos registros de análisis.	**Cumple**
2.6	**POLÍTICAS DE LA CONSOLA DE ADMINISTRACIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFRAESTRUCTURA, EL PRODUCTO DEBE OFERTAR:**	**Cumple**
2.6.1	Capacidad para aplicar políticas basadas en la ubicación y basadas en el usuario registrado.	**Cumple**
2.6.1	Capacidad para aplicar varias políticas a un único punto final, pero solo una activa a la vez.	**Cumple**
2.6.1	Capacidad para aplicar una política a un grupo de puntos finales.	**Cumple**
2.6.1	Una plantilla única para cada servicio de seguridad.	**Cumple**
2.6.1	Cada servicio de seguridad deberá tener su plantilla de política configurable con opciones específicas para activar / desactivar y configurar funcionalidades como el análisis antimalware, las capacidades de la zona de pruebas en la nube, las opciones de aprendizaje automático, la introspección del hipervisor, el cortafuegos, el control de acceso a la red, la inclusión en la lista blanca de aplicaciones, la lista negra de aplicaciones y el acceso a la web, control de dispositivos, ubicación de dispositivos, aplicación de autenticación y acciones a tomar en caso de malware y dispositivos no compatibles detectados, como bloqueo remoto, desbloqueo, borrado y cifrado SD.	**Cumple**
2.7	**INFORMES GENERADOS POR LA CONSOLA DE ADMINISTRACIÓN:**	**Cumple**
2.7.1	Debe permitir como mínimo generar informe global, por modulo, informe de ataques, informe de comportamiento de usuario, usuarios más atacados y otros.	**Cumple**
2.7.2	Debe permitir generar informe programados, para ser enviados por correo a cualquier número de destinatarios (sin necesidad de tener una cuenta en la consola).	**Cumple**
2.7.3	Debe permitir generar filtros para informes programados para recibir por correo únicamente información relevante para cada usuario.	**Cumple**
2.7.4	Debe permitir exportar el resumen a archivo .pdf, detalles a archivo .csv.	**Cumple**
2.8	**CUARENTENA**	**Cumple**
2.8.1	Debe permitir restauraciones remotas, con ubicación configurable y borrar.	**Cumple**
2.8.2	Debe permitir centralizar la cuarentena para archivos infectados.	**Cumple**

2.8.3	Descargar archivos, disponibles solo para máquinas virtuales integradas con vShield o NSX.	**Cumple**
2.8.4	Debe permitir personalizar la hora en que los archivos se almacenan en cuarentena hasta por 180 días.	**Cumple**
2.9	**USUARIOS**	**Cumple**
2.9.1	La administración de los usuarios debe estar basada en roles. Múltiples tipos predefinidos: root, administrador, reporte o usuario personalizado. a. Root: gestiona los componentes de la solución. b. Administrador: gestiona los servicios de seguridad. c. Reporte: monitorea y crea informes.	**Cumple**
2.9.2	Debe permitir importar la lista de usuarios desde Microsoft Active Directory (la autenticación AD se usará para iniciar sesión).	**Cumple**
2.9.3	Debe permitir la configuración detallada de los derechos de destino administrativos, para seleccionar qué servicios y objetos puede administrar un usuario. Cierre de sesión automático para cualquier tipo de usuario para mayor seguridad con respecto a la información que se muestra en la consola de administración.	**Cumple**
2.10	**LOGS**	**Cumple**
2.10.1	Debe permitir el registro las acciones del usuario para su cumplimiento.	**Cumple**
2.10.2	Debe permitir el registro detallado para cada acción del usuario.	**Cumple**
2.10.3	Debe permitir hace búsquedas complejas.	**Cumple**
2.11	**CERTIFICADOS DE SEGURIDAD**	**Cumple**
2.11.1	El acceso a la consola de administración debe estar protegido por certificado (https).	**Cumple**
2.11.2	El servidor web, desde la consola de administración central, debe permitir la importación de certificados digitales emitidos por una autoridad de certificación con licencia o por su propia organización. Importar certificados para que sea intuitivo y hecho desde la consola de administración central.	**Cumple**
2.11.3	La gestión y la comunicación con dispositivos móviles (iOS) deben realizarse de forma segura, a través de certificados digitales. Estos certificados serán firmados por una Autoridad de Certificación autorizada o por su propia organización.	**Cumple**
2.11.4	Le permite importar la cadena de certificados de PKI (infraestructura de clave pública) El oferente deberá entregar diagrama de red con la conexión previa y final de IP.	**Cumple**
2.11.5	Debe admitir claves de cifrado de certificado digital con una longitud mínima de 1024 bits.	**Cumple**
2.11.6	Los certificados digitales, una vez importados, deben ser reemplazables en caso de que caduquen o sean revocados.	**Cumple**
2.11.7	Los certificados aceptados en el proceso de importación deben estar en formato pfx o p12 y protegidos por una contraseña.	**Cumple**
2.11.8	La solución debe ser capaz de generar certificados digitales por sí misma.	**Cumple**
2.11.9	La solución debe poder mostrar en la consola central información sobre los certificados: nombre, autoridad de emisión, fecha de emisión y fecha de vencimiento de los certificados emitidos.	**Cumple**
2.12	**ACTUALIZACIONES**	**Cumple**
2.12.1	La solución debe permitir la prueba de nuevos kits o actualizaciones de productos en un entorno cerrado.	**Cumple**
2.12.2	La solución debe tener la capacidad de decidir qué kits se publicarán en la red.	**Cumple**

2.12.3	La solución debe poder definir y aplicar diferentes políticas para los puntos finales críticos de producción y actualizarlos después de que se haya probado el nuevo paquete.	**Cumple**
2.12.4	La solución debe poder desactivar la opción de clasificación.	**Cumple**
2.12.5	La plataforma de ensayo debe entregarse como un dispositivo virtual.	**Cumple**
2.12.6	El servidor de actualización puede actuar como una puerta de enlace para los datos.	**Cumple**
2.12.7	La consola y la plataforma de pruebas deben poder descargar automáticamente nuevos kits.	**Cumple**
2.12.8	La consola debe poder configurar el número máximo de kits que puede almacenar.	**Cumple**
2.12.9	La opción de organización puede definir varios anillos de actualización para aplicar actualizaciones de productos.	**Cumple**
2.13	**ACTUALIZACIONES OFFLINE**	**Cumple**
2.13.1	La solución puede usar actualizaciones fuera de línea en una infraestructura aislada.	**Cumple**
2.13.2	Las actualizaciones se pueden recuperar y transferir a través de USB HDD / USB Stick, File Server, FTP	**Cumple**
2.14	API´s	**Cumple**
2.14.1	La solución debe permitir a los administradores utilizar la llamada a la API.	**Cumple**
2.14.2	La solución debe incluir métodos para administrar cuentas de usuario, configurar notificaciones, administrar grupos, carpetas y puntos finales, administrar políticas, generar informes a través de APIs.	**Cumple**
3	**PROTECCIÓN PARA ESTACIONES DE TRABAJO Y SERVIDORES FISICOS Y/O VIRTUALIZADOS Y DISPOSITIVOS MOVILES**	**Cumple**
3.1	**CARACTERÍSTICAS MÍNIMAS**	**Cumple**
3.1.1	La existencia de un único motor antimalware.	**Cumple**
3.1.2	Para minimizar el consumo de recursos, los productos antimalware deben permitir la instalación de módulos personalizados (por ejemplo, la instalación del producto antimalware sin el módulo de control de acceso web o sin el módulo Firewall).	**Cumple**
3.1.3	Agente y consola únicos: Una solución de agente y consola únicos (desarrollado desde ceros), que incorpora todas las tecnologías necesarias para proteger eficazmente los endpoints empresariales y detener todas las amenazas digitales. Elimina la necesidad de ejecutar varios agentes y simplifica significativamente la implementación y la operativa.	**Cumple**
3.2	**REQUISITOS DEL SISTEMA:**	**Cumple**
3.2.1	Sistemas operativos para estaciones de trabajo: Windows 10 o superior, Windows 8.1, Windows 8, Windows 7.	**Cumple**
3.1.2	Tabletas y sistemas operativos integrados: Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7, Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded con Service Pack 2, Windows XP Tablet PC Edition.	**Cumple**
3.1.3	Sistemas operativos dispositivos móviles: Apple iPhone y tabletas iPad (iOS 8.1+) • Google Android smartphones y tabletas (4.1+)	**Cumple**
3.3	**LA SOLUCIÓN DE EDR DEBERÁ ESTAR EN INCLUIDA EN EL MISMO AGENTE DE EL ANTIVIRUS Y DEBERÁ PROVEER MÍNIMO LAS SIGUIENTES FUNCIONALIDADES**	**Cumple**

3.3.1	Investigación y respuesta ante incidentes: Rápida priorización e investigación de incidentes, con línea de tiempos del ataque y salida en espacio aislado, permite que los equipos de respuesta ante incidentes reaccionen rápidamente y detengan los ataques en curso (respuesta con un solo click).	**Cumple**
3.3.2	Análisis integrado de riesgos en los endpoints: Analiza continuamente los riesgos utilizando cientos de factores para descubrir y priorizar los riesgos de configuración para todos sus endpoints, lo que permite la adopción automática de acciones de endurecimiento.	**Cumple**
3.3.3	Protección modular por capas: Las tecnologías sin firmas, que incluyen aprendizaje automático avanzado local y en la nube, tecnologías de análisis del comportamiento, espacio aislado integrado y endurecimiento de dispositivos constituyen una protección por capas altamente eficaz contra las amenazas sofisticadas.	**Cumple**
3.3.4	Análisis forense de los ataques de extremo a extremo: La visibilidad del ataque previa y posterior al incidente permite a los analistas de seguridad realizar análisis de causa raíz tanto en ataques bloqueados como en actividades sospechosas en curso.	**Cumple**
3.3.5	Prevención y detección precisas de última generación con reparación automática: El mejor repertorio de medidas de prevención del mundo y sus capacidades de detección basadas en el comportamiento durante la ejecución detienen y evitan la ejecución de las amenazas avanzadas en la infraestructura de la empresa. Una vez que se detecta una amenaza activa, se pone en marcha la respuesta automática para bloquear daños posteriores o movimientos laterales.	**Cumple**
3.3.6	SecOps integradas: Incorpora módulos que contribuyen a reducir la brecha entre la TI y las operaciones de seguridad. Disminuye el esfuerzo operativo necesario para minimizar el riesgo digital al reducir la superficie de ataque: control de apps, control de dispositivos y administración de parches.	**Cumple**
3.3.7	Agente y consola únicos: Una solución de agente y consola únicos (desarrollados desde ceros), que incorpora todas las tecnologías necesarias para proteger eficazmente los endpoints empresariales y detener todas las amenazas digitales. Elimina la necesidad de ejecutar varios agentes y simplifica significativamente la implementación y la operación.	**Cumple**
3.3.8	Cobertura multiplataforma y API de integración de terceros: Cubre todos los endpoints empresariales que ejecuten Windows, Linux o Mac, en infraestructuras físicas, virtualizadas o en la nube, y proporciona seguridad consistente en toda la infraestructura. Admite la integración con herramientas de operaciones de seguridad preexistentes (SIEMS, como por ejemplo Splunk) y tecnologías específicas de centros de datos (los principales hipervisores del mercado).	**Cumple**
4	**ADMINISTRACIÓN E INSTALACIÓN:**	**Cumple**
4.1	Antes de la instalación, el administrador puede personalizar los paquetes de instalación incluyendo solo los módulos deseados: análisis basado en el comportamiento, cifrado completo del disco, firewall, control de contenido, control de dispositivos, control de aplicaciones, administración de parches.	**Cumple**
4.2	La instalación se puede realizar de varias formas: a. Al descargar el paquete antimalware directamente a la estación de trabajo donde se instalará. b. Mediante la instalación remota, directamente desde la consola web.	**Cumple**
4.3	La instalación en máquinas desde una ubicación remota se realizará utilizando un cliente instalado existente en estas ubicaciones para minimizar el tráfico WAN.	**Cumple**

4.4	La consola de administración informará el número de estaciones de trabajo que tienen el antimalware instalado y el número de estaciones de trabajo que están desprotegidas.	**Cumple**
4.5	La consola de administración incluirá en los paneles / widgets configurables del panel de control.	**Cumple**
4.6	La consola de administración incluirá información detallada sobre las estaciones de trabajo / servidores: nombre, IP, sistema operativo, módulos instalados, política aplicada, información de actualización.	**Cumple**
4.7	La consola de administración permitirá al administrador enviar una política para configurar todo el producto antimalware, tanto para estaciones de trabajo como para servidores.	**Cumple**
4.8	La consola de administración permitirá dos tipos de cuentas, usuario con privilegios de administrador y usuario no privilegiado, este tipo de roles deberán poderse asignar qué grupos de usuarios específicos para determinar quiénes pueden cambiar la configuración en la consola y los agentes y quienes solo podrán generar informes.	**Cumple**
4.9	La consola de administración incluirá una sección de registro donde se mencionarán todas las acciones, con información detallada: iniciar sesión, editar, crear, cerrar sesión, mover.	**Cumple**
4.10	La consola de administración deberá incluir un módulo de parchado de aplicaciones y sistemas operativos que pueda ejecutar tanto parchado virtual como real de las aplicaciones.	**Cumple**
4.4.1	La consola de administración permitirá la posibilidad de crear un paquete único, utilizado para sistemas operativos de 32 bits y de 64 bits, MAC y Linux.	**Cumple**
5	**LAS PRINCIPALES CARACTERÍSTICAS Y FUNCIONALIDADES DEL ANTIMALWARE Y EL MÓDULO ANTISPYWARE:**	**Cumple**
5.1	El administrador de la solución puede configurar el escaneo automático en tiempo real para que no analice archivos o archivos con un tamaño mayor que "x" MB.	**Cumple**
5.2	El escaneo automático en tiempo real puede admitir escanear archivos con hasta 16 niveles de profundidad.	**Cumple**
5.3	Escaneo heurístico del comportamiento y monitoreo de procesos.	**Cumple**
5.4	Escaneo en la nube y tecnología de aprendizaje automático.	**Cumple**
5.5	Tecnología anti-ransomware y anti-exploit.	**Cumple**
5.6	Capacidad para detectar ataques sin archivos, incluidos aquellos que utilizan herramientas legítimas del sistema operativo, como Powershell o intérpretes de scripts. La solución no debe bloquear globalmente los scripts para lograr esto.	**Cumple**
5.7	Capa de seguridad adicional de próxima generación, basada en heurísticas agresivas y tecnología de aprendizaje automático, para detectar y bloquear la nueva generación de ataques avanzados o dirigidos y malware sofisticado antes de la ejecución. Debe proporcionar: a.Clasificación de los tipos de ataque. b. Posibilidad de informar únicamente sobre amenazas detectadas, sin bloquearlas. c. Capacidad para ajustar la agresividad de detección para cada categoría de ataque, con opciones para tomar medidas en detecciones de mayor confianza y también informar todas las demás detecciones de menor confianza. Al menos 3 niveles de detección estarán disponibles. d. Capacidad para realizar diferentes acciones sobre los archivos detectados y las amenazas basadas en la red.	**Cumple**

5.8	Escaneo bajo demanda y en acceso de cualquier medio de almacenamiento de información (CD, discos duros externos, disco compartido). Además, el proceso de exploración se puede detener si los dispositivos de medios de almacenamiento contienen información de más de "x" MB.	**Cumple**
5.9	Escaneo automático de correos electrónicos a nivel de estación de trabajo, independientemente del cliente de correo electrónico, para los protocolos SMTP y POP3.	**Cumple**
5.10	Configuración de las rutas a escanear, hasta el nivel de archivo.	**Cumple**
5.11	La solución debe proporcionar Exclusiones incorporadas para roles de servidor de Microsoft (DNS, DHCP, AD, Exchange, Sharepoint).	**Cumple**
5.12	El producto antimalware permitirá definir la lista de exclusión del análisis, tanto para el análisis "en acceso" como para el análisis "a pedido", para ciertas carpetas, discos, archivos, extensiones o procesos.	**Cumple**
5.13	Con una base de datos completa de firmas de spyware y detección heurística de estos programas, el producto tendrá que ofrecer protección antispyware.	**Cumple**
5.14	Para no sobrecargar los recursos del sistema, el producto antimalware debe contener un solo motor de análisis. Podrá ejecutar exploraciones programadas con baja prioridad y puede apagarse automáticamente después de explorar la estación de trabajo.	**Cumple**
5.15	Para una mayor protección, antimalware debe tener 4 tipos de detección: basada en firmas, basada en heurísticas, procesos de monitoreo continuo y escaneo en la nube.	**Cumple**
5.15	Para una mayor protección, antimalware debería poder escanear HTTP y SSL también.	**Cumple**
5.17	Para una mejor administración del antimalware instalado en las estaciones de trabajo, el producto incluirá la opción de establecer una contraseña para la protección de la desinstalación.	**Cumple**
5.18	Para la seguridad del usuario, el cliente incluirá un módulo antiphishing que tendrá la opción de verificar los enlaces buscados con los motores de búsqueda (Asesor de búsqueda).	**Cumple**
5.19	La aplicación antimalware debería ofrecer acceso para el sistema operativo Linux.	**Cumple**
5.1	**FIREWALL:**	**Cumple**
5.1.1	El módulo se puede instalar / desinstalar de acuerdo con las preferencias del administrador.	**Cumple**
5.1.2	Se debe permitir bloquear el análisis de puertos.	**Cumple**
5.1.3	Se debe permitir o denegar la conexión compartida a internet.	**Cumple**
5.1.4	Capacidad de mostrar o no notificaciones cuando se une un nuevo equipo a la red Wifi	**Cumple**
5.1.5	Capacidad de tener un sistema de detección de intrusos IDS tuneable.	**Cumple**
5.1.6	Debe permitir aplicar perfiles basados en nivel de confianza (De confianza, Hogar/Oficina, Publico, Insegura, Dejar que decida Windows)	**Cumple**
5.1.7	Capacidad de realizar reglas para aplicaciones y conexiones	**Cumple**
5.1.8	Debe permitir los siguientes protocolos (TCP,UDP, 3PC,A/N,AH,ARGUS, ARIS,AX.25,BNA,BBC-RCC-MON,BNA,BR-SAT-MON, CBT,CFTP,CHAOS,CPHB,CPNX,CRTP,CRUDP,DCCP,DDP,DDX,DGP,EGP,EIGRP,EMCON,ENCAP,ESP, ETHERIP,FC,FIRE,GGP,GMTP,GRE,HIP,HMP,I-NLSP,IATP,ICMP,IDRP,IDRP-CMTP,IFMP,IGMP,IGP,IL,IPCV,IPcomp,IPIP,IPLT,IPPC,IPTM,IPX-in-IP,IPV6-	**Cumple**

	FRAG,IPV6-ICMP,IPV6-NONXT,IPV6-OPTS,IPV6-ROUTE,IRTP,ISO-IP,ISO-TP4,KRYPTOLAN,L2TP,LARP,LEAF-1,LEAF-2,MANET,MERIT-INP,MFE-NSP,MHRP,MICP,MOBILE,MTP,MUX,NARP,NETBLT,NSFNET-IGP,NVP-II,OSPF,PGM,PIM,PIPE,PNNI,PRM,PTP,PUP,PVP,QNX,RDP,RSVP,RVD,SAT-EXPAK,SAT-MON,SCC-SP,SCPS,SCTP,SDRP,SECURE-VMT).	
5.2	**CONTROL DE USUARIO:**	**Cumple**
5.2.1	Debe permitir el bloqueo del acceso a Internet para clientes específicos o grupos de clientes.	**Cumple**
5.2.2	Debe permitir el bloqueo del acceso a ciertas aplicaciones.	**Cumple**
5.2.3	Debe permitir el bloqueo del acceso a internet por ciertos periodos de tiempo.	**Cumple**
5.2.4	Debe permitir el bloqueo de páginas web que contengan determinadas palabras clave.	**Cumple**
5.2.5	Debe permitir el bloqueo del acceso a páginas web específicas especificadas por el administrador.	**Cumple**
5.2.6	Debe restringir el acceso a ciertos sitios web por algunas categorías predeterminadas (por ejemplo, citas en línea, violencia, etc.).	**Cumple**
5.3	**CONTROL DE DISPOSITIVOS:**	**Cumple**
5.3.1	Debe prevenir la fuga de datos confidenciales y las infecciones de malware a través de dispositivos conectados.	**Cumple**
5.3.2	De permitir la aplicación de reglas de bloqueo y exclusiones a través de políticas a una amplia gama de dispositivos y tipos.	**Cumple**
5.3.3	Debe enviar información como el nombre del dispositivo, ID de clase, fecha y hora de conexión.	**Cumple**
5.3.4	Debe tener tipos predefinidos de dispositivos como: CDROM, dispositivos de imagen, unidades de cinta, puertos COM / LPT, incursión SCSI, impresoras, NIC, almacenamiento interno y externo, etc.	**Cumple**
5.3.5	Debe permitir admitir diferentes configuraciones y privilegios como Permitido, Bloqueado o Personalizado	**Cumple**
5.3.6	Debe permitir el modo de solo lectura para dispositivos de almacenamiento.	**Cumple**
5.3.7	Deber tener la capacidad para bloquear solo el USB y permitir que se utilicen todos los demás puertos.	**Cumple**
5.3.8	Debe permitir la configuración de exclusiones para diferentes tipos de dispositivos.	**Cumple**
5.3.9	Debe permitir el soporte para definir exclusiones de dispositivos: a. Por ID de producto b. Por ID de dispositivo, ID de hardware	**Cumple**
5.4	**ANÁLISIS AUTOMÁTICO DE SANDBOX DE ARCHIVOS SOSPECHOSOS:**	**Cumple**
5.4.1	La solución debe tener la capacidad de realizar un análisis en profundidad de los archivos sospechosos.	**Cumple**
5.4.2	La solución debe tener la capacidad de enviar archivos de forma automática o manual a los servidores de sandbox.	**Cumple**
5.4.3	La solución puede configurarse para permitir que los usuarios accedan a los objetos enviados o bloquearlos hasta que se devuelva el análisis.	**Cumple**
5.4.4	La solución debe permitir diferentes acciones de remediación si un archivo enviado es una amenaza.	**Cumple**
5.4.5	La solución debe tener la capacidad de usar un servidor proxy para el tráfico de la zona de pruebas.	**Cumple**
5.4.6	La solución debe tener la capacidad de detonar archivos individualmente o en grupo.	**Cumple**

5.4.7	La solución debe generar un informe detallado sobre los archivos enviados.	**Cumple**
5.5	**ANTI EXPLOIT AVANZADO.**	**Cumple**
5.5.1	Debe proporcionar protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común.	**Cumple**
5.5.2	Debe tener la capacidad para agregar aplicaciones personalizadas y presentar una lista de aplicaciones predefinidas.	**Cumple**
5.5.3	Debe tener las siguientes técnicas de detección para exploits: • ROP Emulation • ROP Stack Pivot • ROP Illegal Call • ROP Stack Misaligned • ROP Return To Stack • ROP Make Stack Executable • Flash Generic • Shellcode Execution • Shellcode LoadLibrary UNC • Anti-Detour • Flash Payload • ROP Create Thread • Anti-Meterpreter • Obsolete Process Creation • Child Process Creation • Enforce Windows DEP • Enforce Module Relocation (ASLR)	**Cumple**
5.5.4	Las acciones que se deben permitir de acuerdo a cada técnica de detección serán, solo informar o detener proceso.	**Cumple**
5.6	**ADMINISTRACIÓN DEL RIESGO**	**Cumple**
5.6.1	La solución debe proporcionar un módulo para la administración del riesgo que proporcione indicadores de riesgo de todos los endpoints junto con la descripción de cada punto de riesgo y su correspondiente recomendación para mitigar la afectación por configuración.	**Cumple**
5.6.2	Se debe tener la capacidad de resolver características de riesgo de forma automática con un botón de acción.	**Cumple**
5.6.3	La administración de riesgo debe gestionar los diferentes puntos de riesgo a nivel de sistema operativo y a nivel de red.	**Cumple**
5.6.4	Desde la política se debe tener la opción de habilitar o deshabilitar el módulo de Administración del riesgo	**Cumple**
5.6.5	Se tiene que contar con un programador en el cual se gestione el escaneo de riesgos de seguridad por días, semanas y horarios en específico.	**Cumple**
5.6.6	Se debe tener la disponibilidad de una lista de indicadores de riesgos como mínima cantidad de 184 para sistemas operativos y una mínima cantidad de 20 a nivel de red para seleccionar según convenga en el escaneo de seguridad.	**Cumple**
6	**SOLUCIÓN DE SEGURIDAD PARA CORREO OFFICE 365**	**Cumple**
6.1	**CARACTERÍSTICAS GENERALES DE FUNCIONAMIENTO:**	**Cumple**
6.1.1	La solución deberá analizar los correos mediante el patrón tradicional, el atributo del mensaje y la coincidencia de características y adicionalmente deberá complementar dicho análisis con un análisis algorítmico para la detección definitiva de amenazas sin afectar a la precisión	**Cumple**

6.1.2	El análisis de comportamiento por sí solo deberá incluir más de 10.000 algoritmos que analizan más de 130 variables extraídas de cada mensaje de correo electrónico.	**Cumple**
6.1.3	Múltiples motores antivirus basados en la firma y el comportamiento ofrecen protección contra todas las formas de malware, incluidas las variantes de día cero: a. Detección de spam del 99,999% con casi cero falsos positivos b. Protección 100% antivirus	**Cumple**
6.1.4	Un sofisticado motor de políticas que permite al administrador de TI personalizar exactamente cómo fluye el correo electrónico dentro y fuera de la organización. El motor puede inspeccionar todos los aspectos del correo electrónico, incluido el tamaño, el contenido, los archivos adjuntos, los encabezados, el remitente y los destinatarios, y tomar las medidas adecuadas, como deliver, cuarentena, cuarentena de la empresa, redirección, notificación o rechazo.	**Cumple**
6.1.5	La solución avanzada de seguridad de correo electrónico debe contar con un motor de enrutamiento de correo electrónico basado en la nube que permita configurar cuarentenas personales y de empresa con todas las funciones para la administración de mensajes. La categorización profunda(que distingue entre el marketing profesional y los mensajes sospechosos de la campaña de correo electrónico masivo, por ejemplo, permite políticas flexibles que detallan con precisión cómo se procesan y etiquetan los diferentes tipos de mensajes.	**Cumple**
6.1.6	El seguimiento detallado de la edad de desorden es invaluable para los administradores de correo electrónico, lo que les permite ver rápidamente exactamente por qué se entregó o rechazó un correo electrónico, incluidos los encabezados de correo electrónico y la conversación completa con el servidor de correo electrónico remoto.	**Cumple**
6.1.7	La solucion debera ser un Addon al antivirus y debera ser catalogada como una solucion integral para admisnistrarse desde una única consola en la nube	**Cumple**
6.2	Requerimientos mínimos de proteccion:	**Cumple**
6.2.1	Antispam: Varios motores utilizan una combinación de tecnologías para detectar spam, así como ataques de phishing y suplantación de identidad dirigidos más sofisticados.	**Cumple**
6.2.2	Antimalware: Múltiples motores antivirus tradicionales basados en firmas y comportamientos para la detección de malware.	**Cumple**
6.2.3	Protección de tiempo de clic: reescribe direcciones URL en mensajes de correo electrónico y proporciona protección de punto de clic mediante varios servicios de reputación. a. Opciones para autoredirect, haga clic en continue, bloquee la amenaza y muestre/oculte la URL de destino. b. Opción para escanear enlaces en el momento de la entrega del mensaje, así como en el momento del clic.	**Cumple**
6.2.4	Listas seguras y de denegaciones: Cree listas seguras y/o de denegaciones de usuarios individuales y/o de toda la empresa.	**Cumple**
6.2.5	TLS / TLS oportunista: a. Aplique el cifrado TLS y restrinja la comunicación con otros servidores de correo electrónico que no admiten el protocolo TLS. b. Opción para habilitar TLS oportunista con recurrir al texto sin formato si TLS no es compatible con el servidor de correo receptor.	**Cumple**
6.2.6	Autenticación por correo electrónico: Soporte para SPF, DKIM y DMARC.	**Cumple**
6.2.7	Lista de seguimiento ejecutivo: use los detalles sincronizados desde Active Directory para detectar automáticamente los nombres reales de los usuarios	**Cumple**

	dentro de los campos de dirección de encabezado y sobre para protegerse contra ataques de suplantación / fraude de CEO.	
6.2.8	Dominios cercanos (cousin): a. Compara el dominio del remitente con los nombres de dominio legítimos para identificar los dominios cercanos (que varían del nombre de dominio real en uno o dos caracteres). b. Protege contra ataques de suplantación / fraude CEO.	**Cumple**
6.2.9	Etiquetas y encabezados de asunto: a. Agregue etiquetas como [EXTERNAL] o [MARKETING] a las líneas de asunto del mensaje. b. Agregue encabezados HTML o de texto sin formato a los mensajes entrantes que alerten a los usuarios de posibles riesgos.	**Cumple**
6.2.10	Archivos adjuntos: a. Comprobación de tipos MIME de archivos adjuntos con capacidad para bloquear tipos de archivo peligrosos. b. Detectar archivos protegidos con contraseña.	**Cumple**
6.2.11	Listas de palabras clave: crea listas de palabras clave ilimitadas. Utilice reglas para analizar mensajes y tomar medidas basadas en contenido confidencial o confidencial.	**Cumple**
6.2.12	Cola de correo: el correo electrónico se pone en cola automáticamente durante 7 días en caso de error o interrupción del servicio de correo electrónico principal o servidores.	**Cumple**
6.2.13	Supervisión de límites de envío: protección automática contra intentos de enviar grandes volúmenes de mensajes salientes para evitar la lista negra de dominios.	**Cumple**
6.2.14	Prevención del ataque de recolección de directorios (DHA): suelte el correo electrónico destinado a direcciones de correo electrónico no válidas o falsas.	**Cumple**
6.3	**CARACTERÍSTICAS MÍNIMAS DE ADMINISTRACIÓN**	**Cumple**
6.3.1	Motor de directivas: más de 20 desencadenadores condicionales para controlar la entrega de correo electrónico y filtrar los mensajes en función del tamaño, las palabras clave, la puntuación de spam, el tiempo, el origen, el destino, el tamaño de los datos adjuntos, los encabezados, los atributos de AD y mucho más.	**Cumple**
6.3.2	Sincronización de usuarios: el servicio de sincronización de Active Directory garantiza que se repliquen los cambios. Aplique reglas basadas en la pertenencia al grupo de AD si es necesario.	**Cumple**
6.3.3	Interfaz Web: Totalmente gestionada y entregada a través de la consola de GravityZone Email Security.	**Cumple**
6.3.4	Administración delegada: Permite la creación de varios administradores con diferentes niveles de acceso.	**Cumple**
6.3.5	Cuarentena: Opción para mover mensajes a los dientes de cuarentena de empresa y usuario.	**Cumple**
6.3.6	Resumen de cuarentena: los correos electrónicos de resumen enumeran todos los mensajes dentro de la cuarentena del usuario y permiten que los mensajes se previsualicen, publiquen o bloqueen. La interacción con el resumen permite a los usuarios administrar sus listas seguras y denegar individuales. Los usuarios pueden establecer la frecuencia y los días en los que se reciben los correos electrónicos de resumen.	**Cumple**
6.3.7	Descargos de responsabilidad: añada un código descargo de responsabilidad HTML y/o de texto sin formato a todo el correo electrónico saliente. Establezca diferentes descargos de responsabilidad para diferentes dominios.	**Cumple**
6.4	**GESTIÓN DE REPORTES**	**Cumple**

6.4.1	Visibilidad en tiempo real: los gráficos proporcionan una visibilidad detallada del flujo de correo entrante y saliente, así como las reglas activadas y las acciones realizadas. Capacidad para profundizar desde gráficos y gráficos de alto nivel hasta informes detallados.	**Cumple**
6.4.2	Generador de informes: los administradores pueden definir sus propios informes en función de los nombres de campo y los criterios disponibles. Los informes se pueden guardar y luego exportar. Los informes de auditoría se pueden buscar utilizando criterios como el tiempo, el usuario, la dirección del remitente, el asunto, la dirección IP del remitente, el destinatario, la dirección, la acción final, el nombre de la regla. Marcar los informes como 'Favorito" los añade a un área de acceso rápido.	**Cumple**
6.4.3	Programación y alertas: vincule los informes a programaciones y, opcionalmente, solo reciba un informe cuando exista contenido (modo de alerta). Alerta sobre reglas, acciones, contenido, etc.	**Cumple**
6.4.4	Informes de tendencias principales: una selección de informes de tendencias predefinidos con datos de gráficos y tablas. Los informes de tendencias se pueden exportar a PDF y enviarse por correo electrónico a los destinatarios.	**Cumple**
6.4.5	Múltiples vistas: Analizar e informar por tiempo, usuario, dirección del remitente, asunto, IP del remitente, destinatario, dirección, acción final, nombre de la regla.	**Cumple**
6.4.6	Auditoría detallada (seguimiento de mensajes): vista detallada del análisis de mensajes individuales con la razón exacta por la que se entregó o rechazó un correo electrónico. Incluye encabezados de correo electrónico y conversación completa con el servidor de correo electrónico remoto.	**Cumple**
6.4.7	Registro Retención & Autoarchivan: GravityZone Correo electrónico Seguridad Registro Datos Es archivados automáticamente después 90 días y disponible para descargar desde la consola por un período adicional de 12 Meses.	**Cumple**
7	**SERVICIOS PROFESIONALES**	**Cumple**
7.1	El oferente debe contar con acreditación del fabricante como Gold o Platinum. Para lo cual deberá presentar con su oferta la carta de la fabricante dirigida a la Dirección General de Sanidad Militar – DIGSA, donde certifique ser distribuidor autorizado como canal Platinum o Gold, la cual no debe ser mayor a 30 días de expedida. Nota: La DIGSA se reserva el derecho de verificar la autenticidad de las certificaciones aportadas o de solicitar los respectivos contratos o documentos que la soporten, cuando lo considere necesario.	**Cumple**
7.2	El oferente debe contar con mínimo dos (2) ingenieros con certificación como especialista técnico en la solución ofertada, Esta certificación soporta el entrenamiento requerido para realizar labores de configuración, implementación, administración y soporte de la solución ofertada, con tarjeta profesional vigente expedida por el COPNIA o ente certificador de la carrera de ingeniería informática, sistemas o electrónica. Dicha certificación debe ser emitida directamente por el fabricante de la solución, copia de la misma deben ser anexada con la hoja de vida en la oferta presentada; esta certificación se aceptará con una antigüedad de un (01) año al cierre del presente proceso. Los servicios se prestarán en las sedes de la ciudad de Bogotá, dentro de los tiempos establecidos y acordados con la DIGSA.	**Cumple**
7.3	El proveedor de la solución debe estar en la capacidad de suministrar soporte en modalidad 5x8 adicional al soporte que suministra el fabricante.	**Cumple**
	Durante el año de funcionamiento de la solución, el oferente deberá realizar el correspondiente *soporte técnico en sitio* en la Dirección General de Sanidad Militar, una vez que se realice el requerimiento por fallas de funcionamiento del	**Cumple**

	producto de acuerdo al anexo de los "TIEMPOS DE RESPUESTA Y SOLUCIÓN". Adicionalmente a los tickets de soporte se debe realizar una visita de mantenimiento preventivo al mes y entregar el informe respectivo del mantenimiento preventivo realizado a la solución ofertada.	
	El tiempo de solución a los incidentes, fallas y/o errores debe ser de acuerdo al anexo de los "TIEMPOS DE RESPUESTA Y SOLUCIÓN" establecidos a partir del momento en que la DIGSA reporte el error, incidente y/o fallo, bien sea por medio de llamada telefónica o correo electrónico.	**Cumple**
7.4	El proveedor debe hacer la desinstalación de la solución que actualmente tiene la DIGSA y realizar la configuración e instalación de la nueva solución, realizando las configuraciones, actualizaciones, cambios, pruebas y ajustes necesarios para el correcto funcionamiento de la misma hasta nivel usuario final.	**Cumple**
7.5	El proveedor debe dictar capacitación certificada con una intensidad horaria de mínimo 10 horas para 4 funcionarios de la DIGSA, entregando al final de la misma la respectiva certificación.	**Cumple**
7.6	El fabricante deberá contar con soporte en español para atender cualquier caso de soporte que sea escalado en cualquier nivel.	**Cumple**
7.7	El fabricante deberá contar con un servicio de laboratorio de investigación en español para proporcionar de forma rápida actualizaciones de bases de firmas de virus sobre amenazas enfocadas en regiones hispanohablantes.	**Cumple**
7.8	De presentarse una situación de ataque de virus, spam o cualquiera de sus derivados en el ámbito de seguridad de virus, que llegue a afectar la solución informática implementada y los activos informáticos de DIGSA, cubiertos por la solución. El oferente deberá proporcionar todo el recurso humano y tecnológico necesario, el soporte debe ser en las instalaciones de la Dirección General de Sanidad Militar, con un ingeniero o tecnólogo certificado y capacitado, el tiempo para que el ingeniero o tecnólogo, se encuentre en sitio será de acuerdo al anexo (TIEMPOS DE RESPUESTA Y SOLUCIÓN), el cual estará en las instalaciones de la DIGSA hasta la restitución del servicio en un 100% y mitigue el ataque. De lo anterior deberá quedar un informe con la respectiva trazabilidad de la amenaza sufrida, con recomendaciones y soluciones y/o medidas adoptadas para evitar futuros eventos similares. De igual forma programa visitas de monitoreo para verificar la eficacia de la solución suministrada o la necesidad de realizar nuevos ajustes.	**Cumple**
7.9	El oferente deberá entregar un informe mensual detallado con evidencias gráficas (capturas de pantallas, gráficos, reportes y demás), al supervisor del contrato detallando lo realizado durante dicho mes, el informe deberá ser entregado dentro de los primeros cinco (5) días de cada mes.	**Cumple**
7.10	Cada vez que se presente una falla, error, incidencia en la prestación del servicio que haga referencia o que tenga que ver con la solución contratada, el oferente deberá emitir un informe detallado al supervisor del contrato, de lo ocurrido y el paso a paso de cómo se solucionó; este informe deberá ser presentado con evidencias gráficas (capturas de pantallas, graficas, reportes y demás) al día siguiente de la ocurrencia de la falla y/o incidencia y/o error presentado.	**Cumple**
8.	**DOCUMENTACION**	**Cumple**
8.1	El oferente debe entregar con la oferta un cronograma y plan de trabajo propuesto, donde se detallen las actividades de configuración de la consola, instalación, configuración, ajustes, pruebas y puesta en funcionamiento de la solución ofertada, incluyendo la instalación en los servidores y computadores hasta nivel usuario final de la DIGSA.	**Cumple**
8.2	El oferente anexara con la oferta una certificación firmada por el representante legal de la empresa, con fecha de expedición no mayor a 30 días, dirigida a la Dirección General de Sanidad Militar - DIGSA, en donde conste que se brinda la	**Cumple**

	garantía sobre los productos suministrados durante el año de licenciamiento - servicios.	
8.3	El oferente deberá anexar a su oferta los manuales en su última versión de la solución que será instalada, lo cual debe realizarse cada vez que se ejecute cambio de versión, durante la vigencia de los derechos de actualización de la solución.	**Cumple**
8.4	El oferente brindará el soporte técnico de ser requerido en sitio en el horario de 5x8 sin costo adicional, cuando el soporte telefónico o vía e-mail no resuelva los problemas, incidencias y/o errores presentados para el correcto funcionamiento de la solución oferta.	**Cumple**

ANEXO:

TIEMPOS DE RESPUESTA Y SOLUCIÓN EN HORAS CONTINUAS							
Impacto	**Detalle**	**1er Nivel** Mesa ayuda Oferente / soporte en sitio		**2do Nivel** Soporte en sitio oferente / soporte mesa ayuda fabricante		**3er Nivel** Proveedor y fabricante en sitio	
		Atención	**Solución**	**Atención**	**Solución**	**Atención**	**Solución**
	Falla general en la consola que hace imposible administrar la solución de punto final (EDR, parchado de aplicaciones y seguridad para correo office 365)	1 hora	4 horas	1 hora	8 horas	1 hora	24 horas
	Presencia de virus, malware, ransomware, phishing y demás amenazas que afecta el funcionamiento normal de la DIGSA a nivel informático.	1 hora	4 horas	1 hora	8 horas	1 hora	24 horas
Alto	Problema de desconfiguración de algunos servicios de la solución, pero de una manera imperfecta, impacto significativo para la DIGSA, que amenaza aspectos de seguridad futura.	2 horas	6 horas	1 hora	16 horas	1 hora	48 horas
Medio	La solución de punto final (EDR, parchado de aplicaciones y seguridad para correo office 365), continúa funcionando con impedimentos menores. Las tareas pueden continuar con una mínima disminución de performance.	4 horas	8 horas	4 hora	36 horas	2 hora	96 horas
Medio	Deterioro del sistema existente por implementación de la solución de punto final (EDR, parchado de aplicaciones y seguridad para correo office 365)	4 horas	8 horas	4 hora	36 horas	2 hora	96 horas

	Implementación de una solicitud de cambios que no es requerida de manera urgente. Las tareas se desarrollan normalmente.	Planificado con DIGSA	Planificado con DIGSA	Planificado con DIGSA	Planificado con DIGSA	Planificado con DIGSA	Planificado con DIGSA

VERIFICACION EXPERIENCIA PROPONENTES.

EMPRESA	EXPERIENCIA	CUMPLE SI/NO
SOFTICS INGENIEROS SAS	INTERCOLOMBIA SAS	SI CUMPLE
	JEFATURA DE INTELIGENCIA NAVAL	SI CUMPLE
	SOLUCIONES INTEGRALES MJ	SI CUMPLE

- Una vez analizada la experiencia de la propuesta presentada por SOFTICS INGENIEROS S.A.S se puede establecer que cumplen con lo solicitado en el numeral 11.2.2 pliego de condiciones.

FORMULARIO No. 07, CERTIFICACIÓN DE CUMPLIMIENTO
SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO

SOFTICS INGENIEROS SAS CI
SI CUMPLE
Doy fe que a la fecha hemos evaluado y calificado los ítems - Tabla de Valores de los Estándares Mínimos contenidos en el Artículo 27 de la Resolución 0312 de 2019 de acuerdo al número de trabajadores de nuestra organización, con un porcentaje de cumplimiento del 65%. INFORMACION EXTRAIDA DE FORMULARIO No. 6 FIRMADO Y DILIGENCIADO POR EL REPRESENTANTE LEGAL.

- Una vez analizados los formularios presentados por la firma SOFTICS INGENIEROS S.A.S se puede establecer que cumplen con lo solicitado en el formulario No. 06," Seguridad y Salud en el trabajo" SOFTICS INGENIEROS S.A.S.

CUMPLIMIENTO SGSST.

EMPRESA	CUMPLE SI/NO
SOFTICS INGENIEROS SAS	SI

REQUISITOS PONDERABLES

- Una vez analizado y verificado el requisito de ponderación Técnica Adicional por la firma SOFTICS INGENIEROS S.A.S de acuerdo con el formulario publicado en los documentos del proceso, se otorga el siguiente puntaje al oferente que oferto así;

ITEM	CERTIFICACIÓN	CANT	PUNTAJE	SOFTICS INGENIEROS SAS
1	Tres (3) charlas virtuales de una (1) hora, enfocadas a sensibilizar y concientizar a los usuarios finales de la DIGSA, en temas relacionados con seguridad digital (Phishing, virus informáticos, maleare, ingeniería social y medidas de protección)	1	250 PUNTOS	CUMPLE
2	2 meses más de licenciamiento de la solución de protección de punto final que incluya EDR, parchado de aplicaciones y seguridad para correo office 365 para la Dirección General de Sanidad Militar, sin costo alguno para la Entidad (DIGSA).	1	250 PUNTOS	CUMPLE
TOTAL, PUNTOS			**500**	

- Una vez analizado y verificada la evaluación de cumplimiento de la Ley 816 de 2003 "Protección a la Industria Nacional", modificada por el Decreto 019 de 2012 y los artículos 2.2.1.2.4.1.3. y 2.2.1.2.4.2.1 del Decreto 1082 de 2015, de La protección a la industria nacional se le otorga el siguiente puntaje.

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTAJE MÁXIMO
El oferente cuya oferta de bienes y/o servicios de origen 100% nacional, oferentes de bienes y/o servicios provenientes de estados con los cuales Colombia tenga acuerdos comerciales y oferentes de bienes y/o servicios extranjeros que acrediten reciprocidad, de acuerdo con la legislación nacional.	20%

Tratándose de proponentes extranjeros a quienes no les aplique el principio de reciprocidad, pero que incorpore bienes y/o servicios extranjeros acreditados (con componente nacional).	N/A

CONCLUSION: Una vez analizados todos los aspectos técnicos establecidos en el proceso de selección abreviada de menor cuantía No. 129-MDN-COGFM-JEMCO-DIGSA-2021 se establece que el oferente SOFTICS S.A.S este habilitado técnicamente.

AASD.LINDA JASBLEIDY RODRIGUEZ VASQUEZ
COMITÉ TECNICO EVALUADOR
GRUPO SISAM

DIGSA