CONTRATO No. 4600096176 DE 2022
PERIODO DE VERIFICACIÓN: DEL 13 AL 31 DE DICIEMBRE DE 2022
FECHA DE ELABORACIÓN DEL INFORME: 13 DE ENERO DE 2023

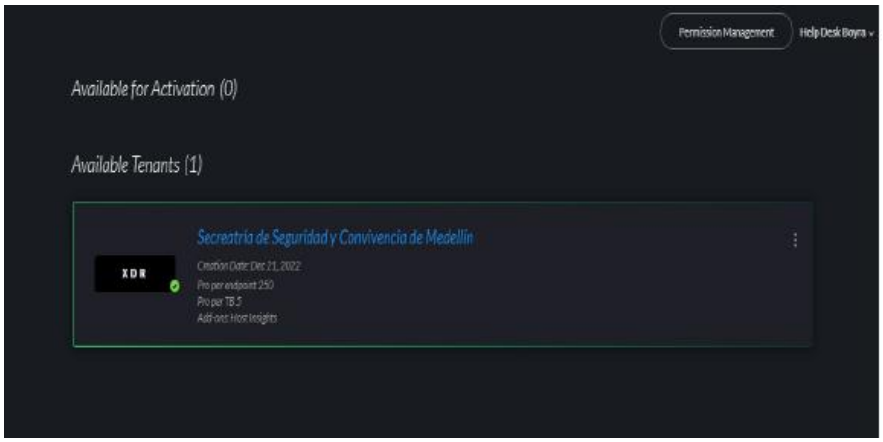
CONTRATANTE:	DISTRITO ESPECIAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN DE MEDELLÍN – SECRETARÍA DE SEGURIDAD Y CONVICENCIA
CONTRATISTA:	BOYRA S.A.
NIT:	830.100.010-4
REPRESENTANTE LEGAL:	LUIS JOSE IGNACIO QUINTERO CUSGUEN
CÉDULA DEL REPRESENTANTE LEGAL:	79.131.510
OBJETO:	ADQUIRIR UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA LA SECRETARÍA DE SEGURIDAD Y CONVIVENCIA.
VALOR INICIAL:	MIL CIENTO SIETE MILLONES DE PESOS M.L ($1.107.000.000) IVA INCLUIDO
ADICIONES:	NO APLICA
VALOR MÁS ADICIONES:	MIL CIENTO SIETE MILLONES DE PESOS M.L ($1.107.000.000) IVA INCLUIDO
DURACIÓN INICIAL:	DESDE EL INICIO DEL CONTRATO EN EL SECOP II, HASTA EL 31 DE DICIEMBRE DE 2022.
AMPLIACIONES:	NO APLICA
SUSPENSIONES:	NO APLICA
DURACIÓN DESPUÉS DE AMPLIACIONES:	DESDE EL INICIO DEL CONTRATO EN EL SECOP II, HASTA EL 31 DE DICIEMBRE DE 2022.
FECHA DE INICIO:	13/12/2022
FECHA DE TERMINACIÓN:	31/12/2022

- Automatización: La plataforma debe permitir la automatización de procesos que permitan confirmar rápidamente la existencia de ataques, con alertas que contengan información detallada que permita investigar y entender la causa raíz de los ataques sin necesidad de contar con años de experiencia.

  Se requiere una solución de seguridad informática XDR (extended detection and response por sus siglas en inglés) capaz de detectar, responder y neutralizar las amenazas informáticas en la red del SIES- M, con capacidad de clasificar los incidentes y acciones de respuesta. Todo el licenciamiento debe ser provisto por un término no inferior a 3años.

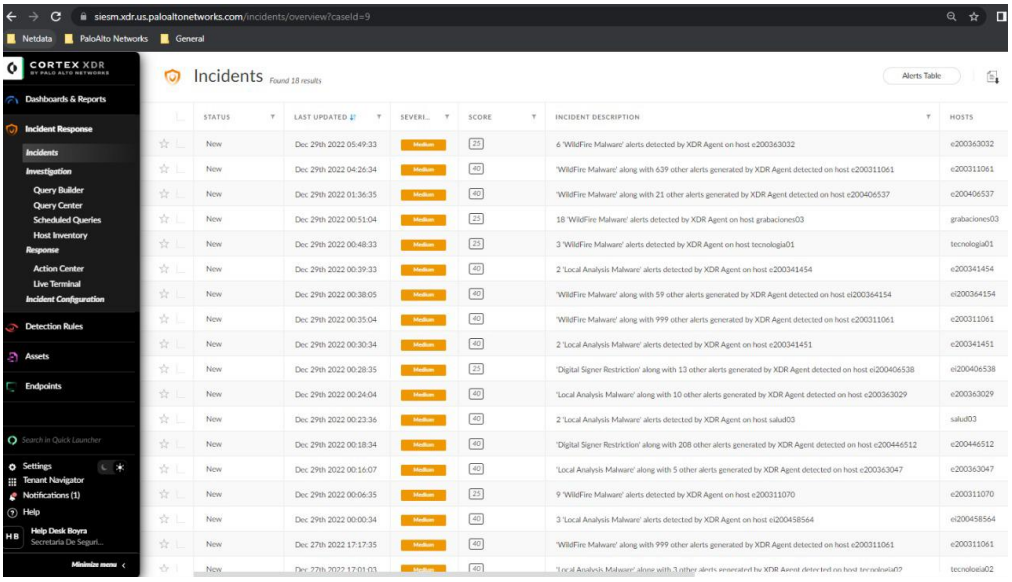
  Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial, que incluya IPS, control de aplicaciones, filtrado de contenido, antimalware, Antispyware y control de amenazas de día cero, control de archivos, calidad de servicio basado en aplicación y VPN (client-to-site y site-to-site) con validación de postura para dispositivos finales.

  Si cumple



- Tenant ID: Secretaría de Seguridad y Convivencia de Medellín
- URL: siesm.xdr.us.paloaltonetworks.com
- Tenant Status: Active
- Región: United States - Americas
- Cortex Data Lake: Secretaria De Seguridad y Convivencia De Medellín
- Serial Number:0220980000020933
- Licenciamiento:
- Pro per endpoint 250
- Pro per TB 5
- Add-ons: Host Insights

1.1. Se requiere de una solución de seguridad XDR que sea capaz de detectar ataques y dar respuestas de los mismos, integrando información de terceros, de la nube, de dispositivos finales y de la red.



1.3. El XDR debe tener la capacidad de prevenir amenazas y bloquear su ataque sin requerir una intervención de un operador externo, es decir, debe tener la capacidad de poder responder a amenazas de manera automática.

Si cumple

1.4. El XDR debe tener capacidad para analizar y realizar correlación de eventos automáticamente, generando una base de conocimiento de los comportamientos en la entidad, lo cual le permita responder ante ataques sofisticados.

Si cumple

1.5. Debe incluir la capacidad de realizar un análisis de los ataques identificando su causa raíz.

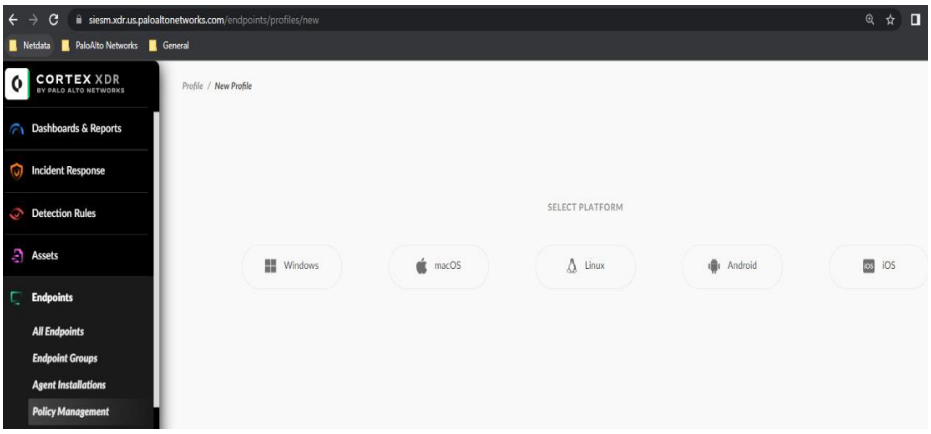
Si cumple

1.6. La solución debe incluir al menos la capacidad de detección, de prevención de amenazas de manera automática, capacidad de investigar y analizar el ataque sufrido, y responder a dicho ataque.

Si cumple

1.7. La solución ofertada debe incluir para la prevención, la detección de al menos exploits, malware, ransomware y ataques sin archivos, sin emplear firmas o parchado virtual. Esta solución debe ser capaz de realizar prevenciones de este tipo en sistemas operativos Windows, Linux, MacOS.

Si cumple

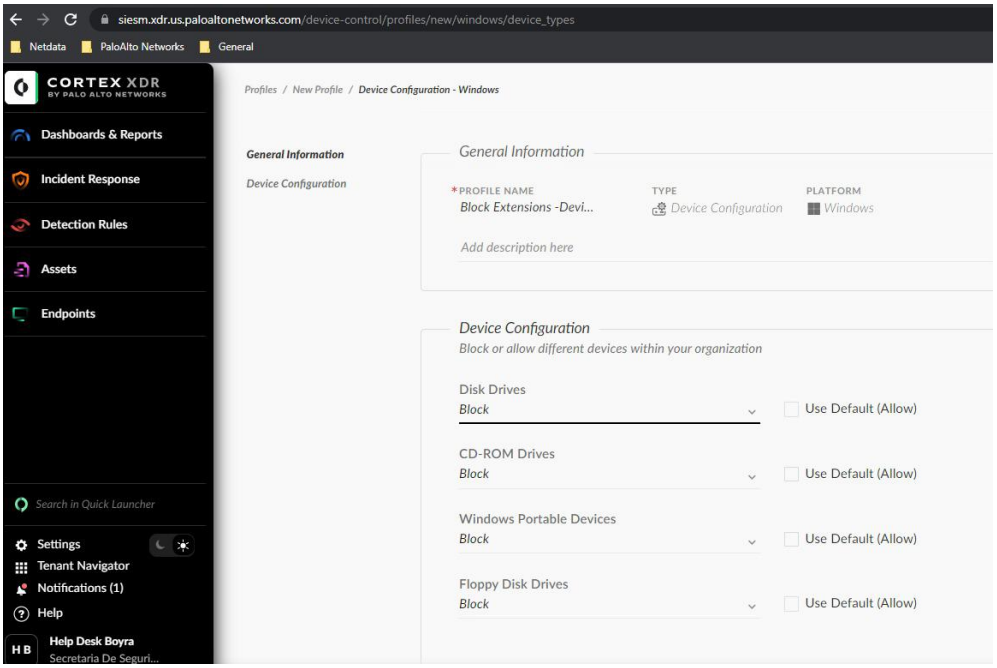


1.8. Debe incluir la capacidad de examinar el comportamiento de procesos relacionados, con el fin de descubrir posibles ataques a medida que estos se produzcan.

Si cumple

1.9. La solución propuesta debe incluir la capacidad de control de dispositivo para el acceso de USB, que permita asignar políticas basadas en grupo, en el directorio activo, restringiendo el uso por el tipo de dispositivo y capacidad de asignar excepciones a las políticas de solo lectura.

Si cumple



1.10. Debe incluir la capacidad de controlar las comunicaciones entrantes y salientes en los dispositivos finales ya sean con sistemas operativos Windows, Linux, MacOS.

Si cumple

1.11. Debe incluir la capacidad de aplicar cifrado y descifrado en los dispositivos finales ya sea por creación de reglas y políticas de cifrado (sean BitLocker o FileVault).

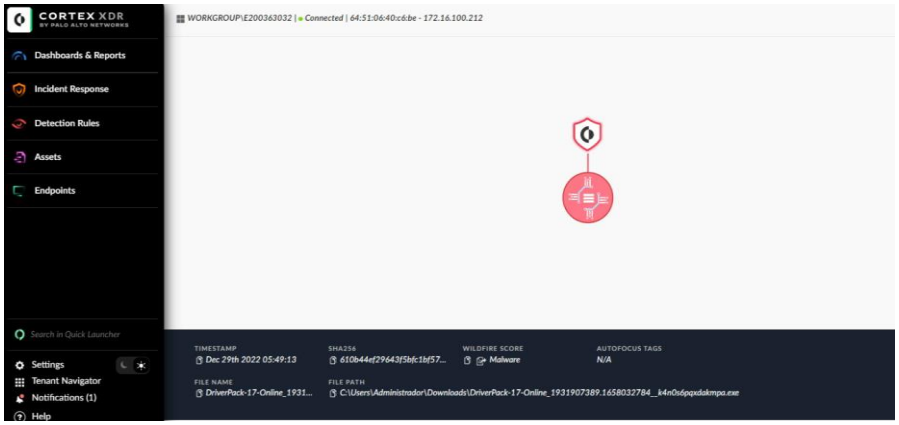
Si cumple

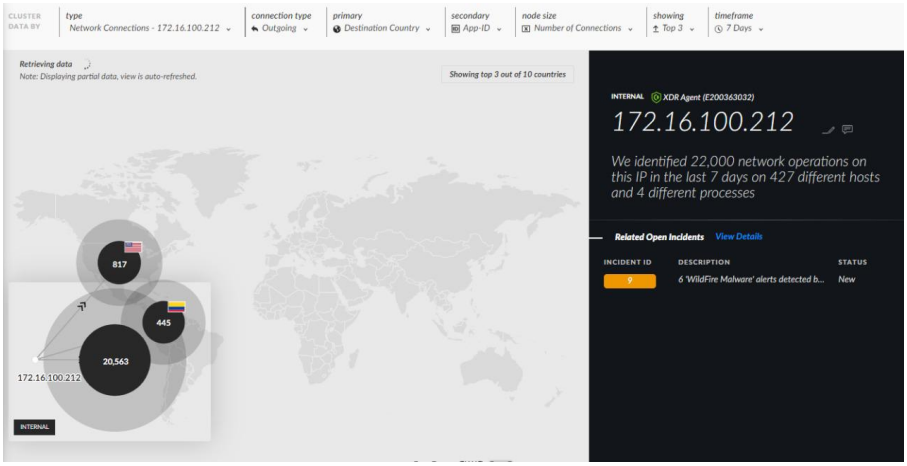
1.12. Debe incluir funcionalidades de visibilidad completa de los dispositivos finales que se hayan cifrado (sean BitLocker o FileVault)

Si cumple

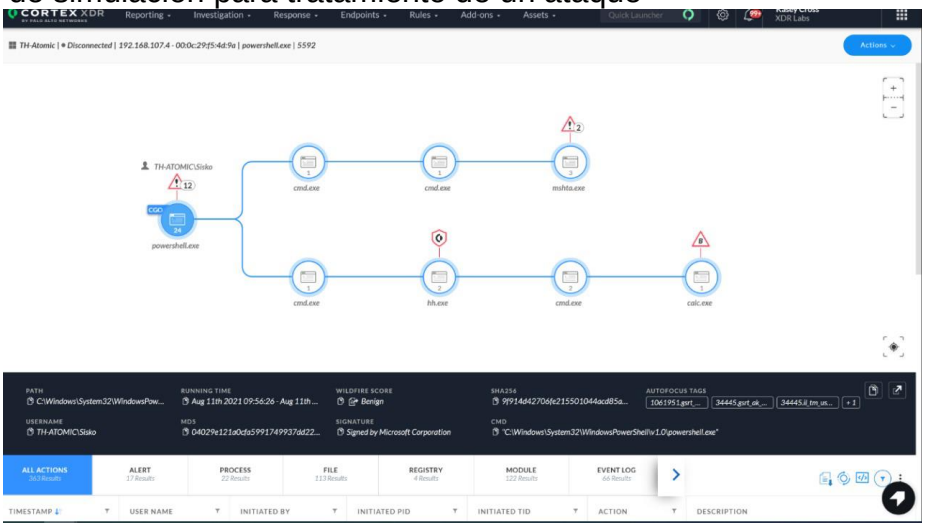
1.13. Se debe incluir la capacidad verificar que las amenazas identificadas sean detenidas y que no se hayan extendido a otros dispositivos (movimiento lateral).

Si cumple





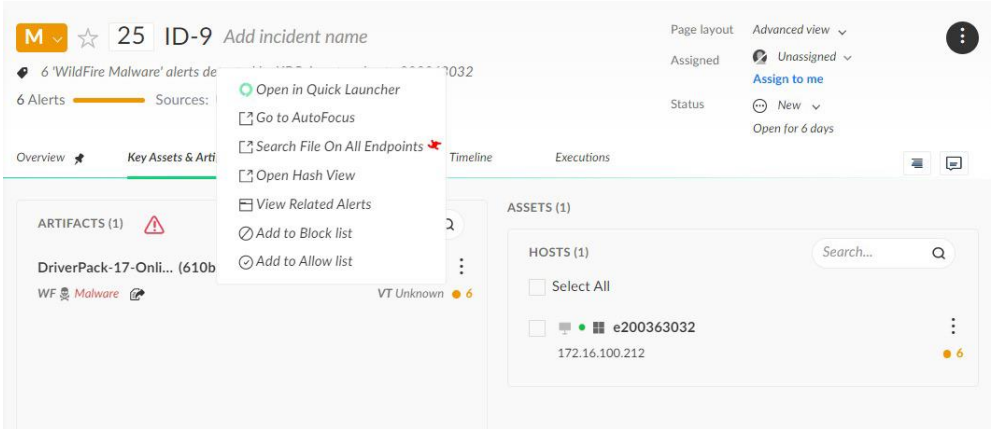
Ejemplo de simulación para tratamiento de un ataque



Centro Administrativo Distrital – CAD – Calle 44 No. 52 – 165
Línea Única de Atención a la Ciudadanía 44 44 144
www.medellin.gov.co
Medellín - Colombia

1.14. La solución debe ser capaz de buscar y erradicar amenazas en todos los dispositivos.

Si cumple



1.15. Debe poder identificar las brechas de seguridad para mejorar la postura defensiva, proporcionando visibilidad de las configuraciones y los archivos claves de los hosts de Windows, Linux, MacOS.

Si cumple

1.16. Debe contar con la posibilidad de un módulo que en tiempo real visibilice la exposición de vulnerabilidades y niveles de parches en los dispositivos en al menos equipos con sistemas operativos Windows, Linux, MacOS, indicando nivel de gravedad de acuerdo con la NIST (National Vulnerability Database por sus siglas en inglés) o por Microsoft.

Si cumple

1.17. Debe poder rastrear al menos 1000 dimensiones de comportamiento, incluyendo atributos.

Si cumple

1.18. Debe tener capacidad de detectar anomalías, ya sean de comportamiento de malware, control, movimientos laterales y de filtración de datos.

Si cumple

1.19. Debe ser capaz de descubrir amenazas evasivas, de manera que se puedan activar alertas basadas en indicadores de compromiso, deben incluir indicadores de comportamiento de peligro.

Si cumple

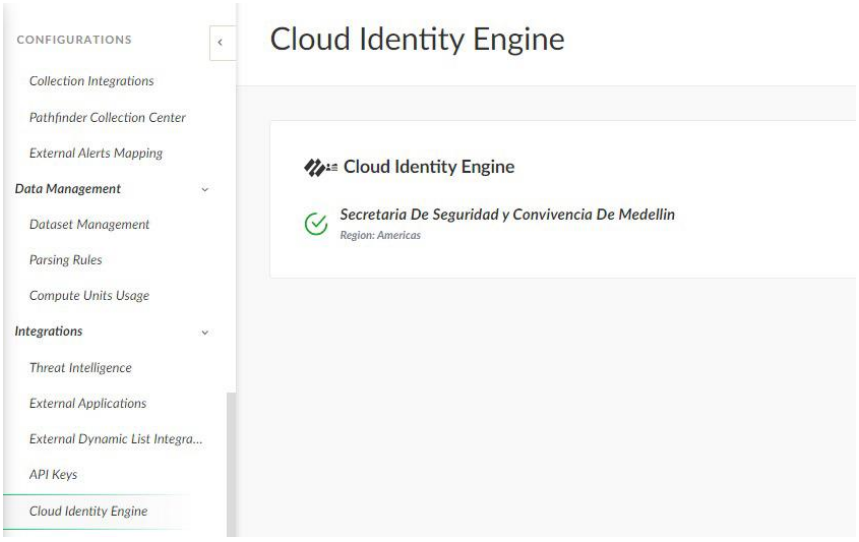
1.20. Debe ser capaz de identificar el uso indebido de sistemas y aplicaciones.

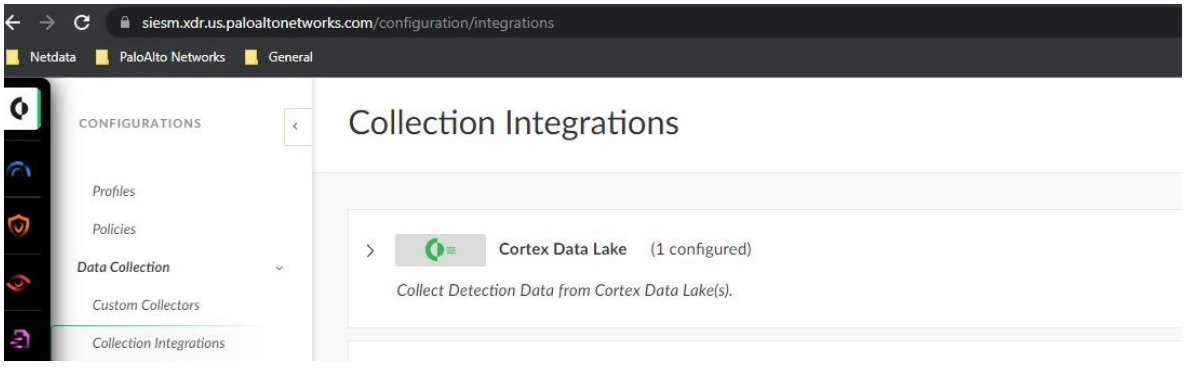
Si cumple

1.21. Debe detectar los ataques de día cero que usen las técnicas de evasión.

Si cumple

1.22. Debe supervisar múltiples características del tráfico de red y clasificar cada dispositivo por tipo (p. ej., computadora, dispositivo Apple iPhone o escáner de vulnerabilidades).





Si cumple

1.23. La solución debe ser capaz de realizar inspección de metadatos a nivel de protocolo en los logs de tráfico, logs de aplicaciones mejorados y los logs de amenazas que sean recopilados del Firewall.

Si cumple

1.24. Debe incluir la capacidad de examinar los datos de los endpoints o puntos finales, alertas de terceros y datos de logs.

Si cumple

1.25. Se debe poder crear perfiles basados en dimensiones de comportamiento, incluyendo frecuencia de conexión, fuente y destino del tráfico y protocolos utilizados.

Si cumple

1.26. El XDR debe contar con una retención de datos de datos de al menos 60 días.

Si cumple

1.27. El XDR debe incluir la función de caza de amenazas y búsquedas de comportamientos de ataque, así como indicadores de comportamiento tradicionales sin tener que aprender un nuevo lenguaje de consulta.

Si cumple

1.28. Debe tener capacidad para filtrar los resultados y reducir el número de eventos a revisar.

Si cumple

1.29. La solución propuesta para el análisis de amenazas debe al menos incluir un motor de análisis que permita realizar la visualización de la secuencia del ataque hasta la causa raíz, también debe incluir la visualización en línea de tiempo de la actividad de los ataques proporcionando información para la investigación de incidentes de manera que permita a los investigadores establecer el alcance y el daño del ataque.

Si cumple

1.30. Para la respuesta de amenazas la solución debe ser capaz de eliminar dichas amenazas con al menos: el aislamiento de los dispositivos finales; ejecutar la finalización de procesos; capacidad para bloquear ejecuciones adicionales; colocar archivos maliciosos en cuarentena; eliminar archivos maliciosos del directorio de trabajo; para la investigación es importante tener

la capacidad de recuperar archivos específicos que se están investigando; tener capacidad de acceder directamente a los dispositivos; debe poder integrarse con herramientas de gestión de terceros con API abiertas; encontrar y eliminar archivos en la organización; restaurar hosts a un estado limpio según las sugerencias de corrección.

Si cumple

1.31. Debe incluir la capacidad para realizar evaluaciones e investigaciones para revisar pruebas, buscar amenazas y realizar evaluaciones de vulneraciones desde una sola consola.

Si cumple

1.32. Debe tener la capacidad de realizar una supervisión o monitoreo permanente de los cazadores de amenazas más importantes del mundo.

Si cumple

1.33. Debe ser capaz de operar a través de datos integrados ya sea de dispositivos finales, de la red de la entidad y de la nube.

Si cumple

1.34. Se deben entregar informes detallados sobre amenazas que revelen las herramientas, los pasos y el alcance de los ataques para que pueda erradicarlos.

Si cumple

1.35. Se deben generar informes de impacto que ayuden a estar un paso adelante a las amenazas emergentes.

Si cumple

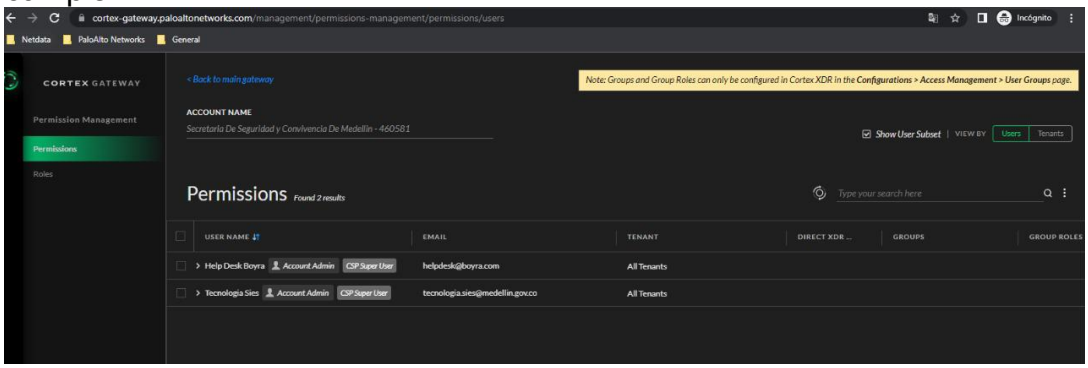
1.36. La solución debe estar en capacidad de sincronizar los datos de seguridad de la entidad.
Si cumple

1.37. Debe ser capaz de recopilar, integrar y normalizar los datos de seguridad de la entidad.

Si cumple

1.38. La solución debe proporcionar controles de privacidad y seguridad para evitar el acceso no autorizado a la información confidencial.

Si cumple



1.39. Debe ser capaz de manejar los datos en tránsito de manera cifrada.

Si cumple

1.40. La solución debe contar con estado de "strategic leader" en el último test de AV comparatives para EPR (Endpoint Prevention and Response).

Si cumple

1.41. La solución debe contar con capacidades:
a. Prevención (sin depender de firmas)
b. Capacidades de EDR (Endpoint Detection and Response, por sus siglas en Ingles) Detección y respuesta de puntos finales.
c. Capacidades de NTA recibiendo información de los Firewall de Nueva Generación “NGFW” (Next Generation Firewall por sus siglas en inglés) con los que cuente la organización.
d. Análisis de Comportamiento de Usuarios y Entidades “UEBA “(User and Entity Behavior Analytics por sus siglas en inglés) Correlación

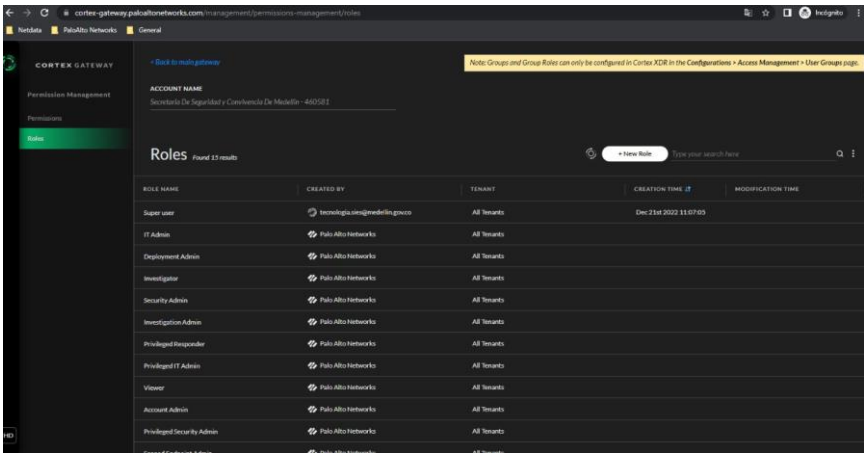
Si cumple

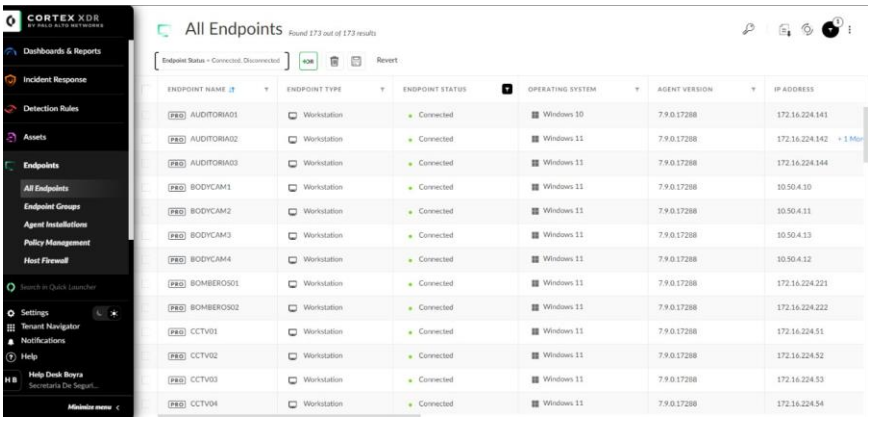
1.42. Debe realizar el análisis de múltiples fuentes: Equipos de la red, equipos terminales, de la nube y datos de terceros.

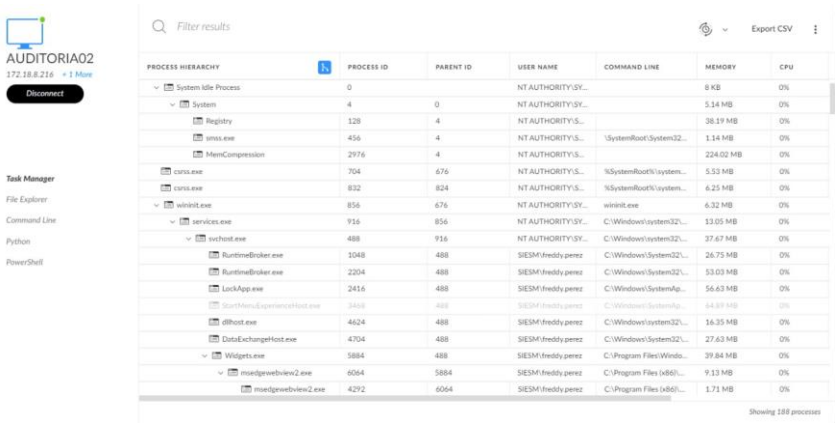
Si cumple

1.43. Debe ser capaz de realizar un inventario de los hosts, que le permite identificar las brechas de seguridad, y que tenga una visibilidad completa de las configuraciones y los archivos claves de los hosts de Windows, Linux, MacOS, siendo capaz de ver la información de los usuarios, grupos, aplicaciones, servicios, controladores, ejecuciones automáticas, recursos compartidos, discos y configuraciones del sistema.

Si cumple

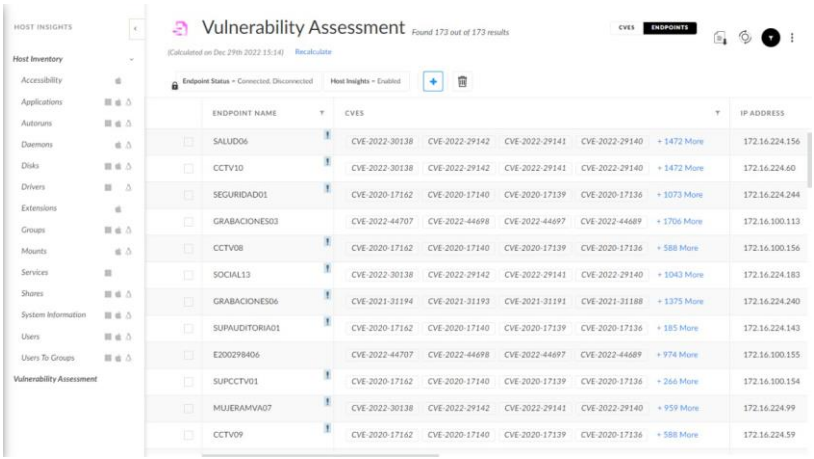

CORTEX GATEWAY
Roles
ROLE NAME
CREATED BY
TENANT
CREATION TIME
MODIFICATION TIME
Super user
IT Admin
Deployment Admin
Investigator
Security Admin
Investigation Admin
Privileged Responder
Privileged IT Admin
Viewer
Account Admin
Privileged Security Admin


CORTEX XDR
All Endpoints
Dashboards & Reports
Incident Response
Detection Rules
Assets
Endpoints
All Endpoints
Endpoint Groups
Agent Installations
Policy Management
Host Firewall
ENDPOINT NAME
ENDPOINT TYPE
ENDPOINT STATUS
OPERATING SYSTEM
AGENT VERSION
IP ADDRESS


AUDITORIA02
Disconnect
Task Manager
File Explorer
Command Line
Python
PowerShell
Filter results
Export CSV
PROCESS HIERARCHY
PROCESS ID
PARENT ID
USER NAME
COMMAND LINE
MEMORY
CPU

1.44. Debe poder revelar las vulnerabilidades en equipos con sistemas operativos Windows, Linux, MacOS, con información actualizada de la gravedad proporcionada por NIST National Vulnerability Database y Microsoft Security Response Center y ser capaz de ver las actualizaciones de la Base de conocimientos (KB) de Microsof Windows instaladas en sus equipos terminales.

Si cumple



1.45. Debe estar en capacidad de analizar los metadatos a nivel de protocolo en los logs de tráfico, los logs de aplicaciones mejorados y logs de amenazas recopilados por los Firewall de Nueva Generación “NGFW” (Next Generation Firewall por sus siglas en inglés) físicos y virtuales

Si cumple

1.46. Debe incluir la capacidad de aprender el comportamiento esperado de usuarios y dispositivos.

Si cumple

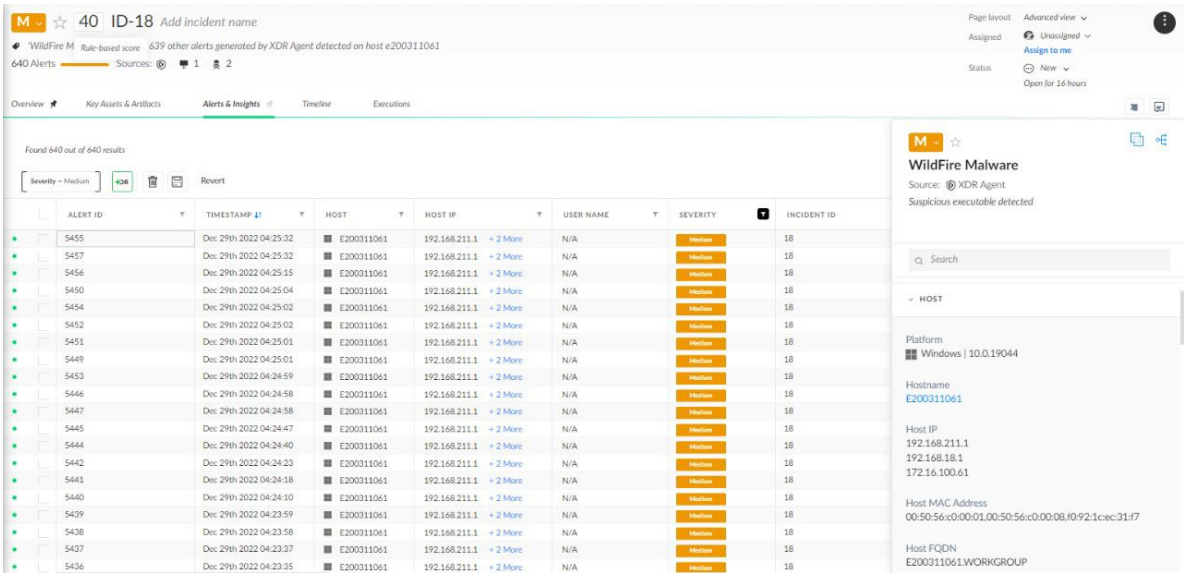
1.47. Debe tener capacidad de retención de datos por al menos 60 días.

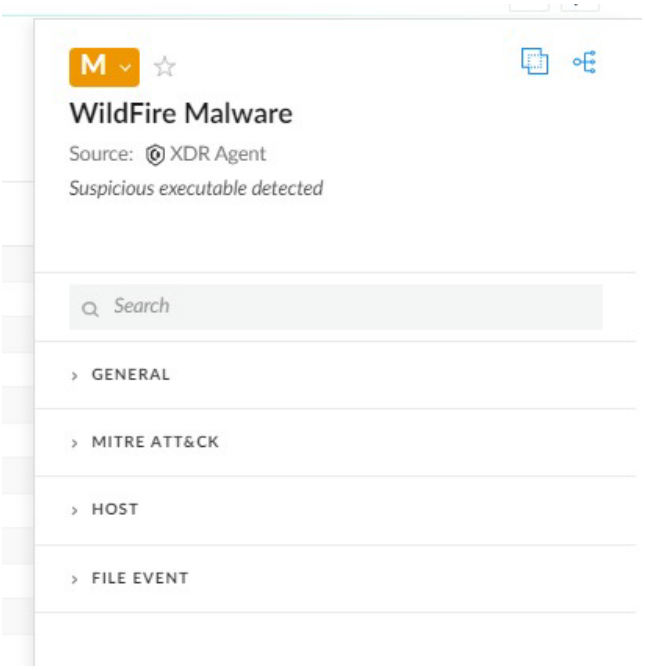
Si cumple

1.48. Debe incluir la capacidad de realizar inspección de datos:
A Nivel de Sesión: IP de origen, IP de destino, puerto de origen, puerto de destino, Bytes enviados y recibidos, Duración de la conexión, Logs de aplicaciones optimizados con datos a nivel transacción en DNS, HTTP, DHCP, RPC, ARP, y ICMP.

A nivel de Información de Usuarios: Usuario registrado, usuario habitual de una máquina, usuario que crea el proceso que inició la comunicación, Grupo de usuarios y unidad organizacional en Directory Sync, Eventos de autenticación de Okta, Azure Active Directory, PingOne, PingFederate, Kerberos y logs de eventos de Windows.

Si cumple





1.49. Debe incluir protección en sistemas operativos en todas las versiones de Windows, Linux, MacOS.

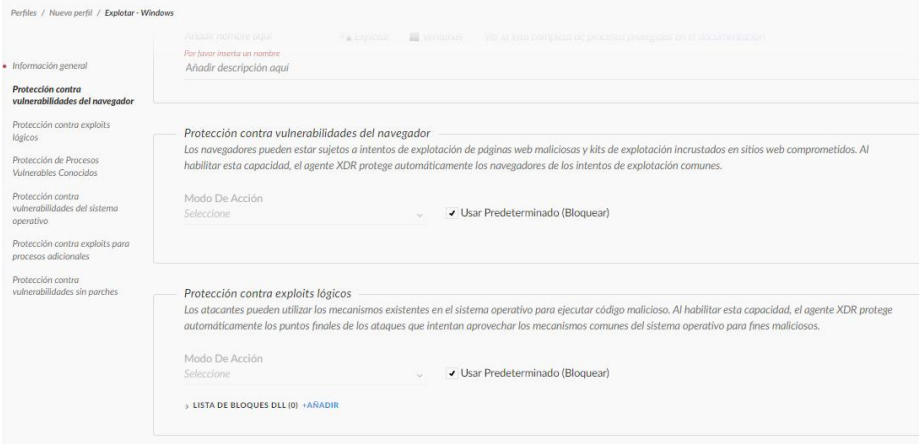
Si cumple

1.50. Debe poder realizar reportes de análisis de sandbox de archivos ejecutados para cualquier archivo PE (Sea de Linux, windows o MacOS) y generar un reporte completo de comportamiento, el reporte debe estar disponible desde la consola de administración.

Si cumple

1.51. Debe incluir la detección de 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, Linux, MacOS.

Si cumple





1.52. Debe tener la capacidad para la Mitigación de vulnerabilidades conocidas, desconocidas y día cero.

Si cumple

1.53. Debe soportar la identificación de distintas técnicas de explotación de vulnerabilidades, entre las que se encuentran Return Oriented Programming, Heap Spray, Jit Spray, Shell link, Structured Exception Handler, etc).

Si cumple

1.54. Debe incluir la protección de aplicaciones contra las técnicas de explotación de manera predeterminada y "out-of-the-box".

Si cumple

1.55. Debe tener entre las aplicaciones predeterminadas: Firefox, Internet Explorer, Microsoft Word, Microsoft Excel, varias versiones de Flash Player, Microsoft Silverlight entre otras.

Si cumple

1.56. Debe tener la Capacidad de utilizar los módulos de protección contra técnicas de explotación en cualquier aplicación o proceso, incluyendo aquellas desarrolladas internamente.

Si cumple

1.57. Debe contar con 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.

Si cumple

1.58. Debe tener la capacidad de configurar perfiles de protección en modo de prevención o monitoreo.

Si cumple

1.59. Debe poder terminar un 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.

Si cumple

1.60. Debe incluir prevención de técnicas de explotación que utilizan Dylib- Hijacking para Mac OS.

Si cumple

1.61. Debe incluir prevención de técnicas de explotación que utilizan ROP para MacOS.

Si cumple

1.62. Debe incluir prevención de técnicas de explotación que utilizan JIT para Mac OS.
Si cumple

1.63. Debe incluir prevención de 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.

Si cumple

1.64. Debe incluir prevención 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.

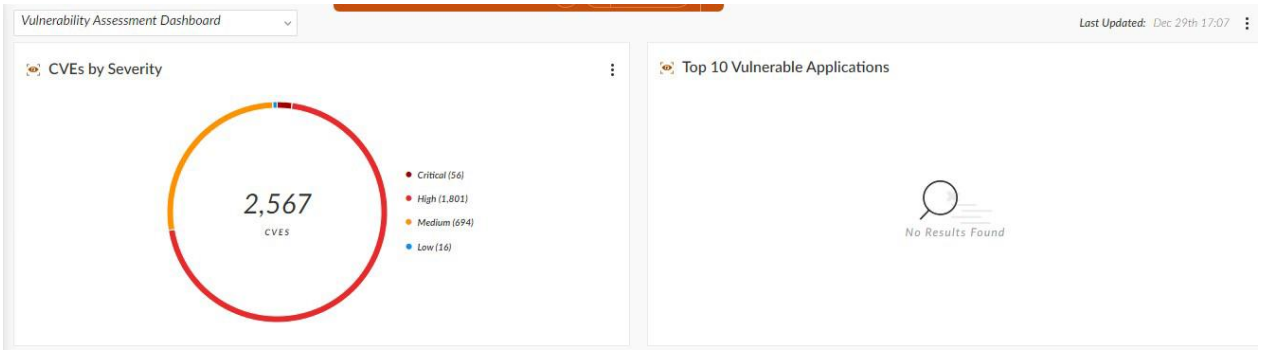
Si cumple

1.65. Debe incluir protección contra webshells de PHP para servidores Linux.

Si cumple

1.66. Debe incluir la capacidad de proporcionar la protección contra la explotación de vulnerabilidades sin necesidad de tener una conexión a la consola.

Si cumple



1.67. Debe ser capaz de identificar y prevenir de intentos de escalar privilegios a nivel de Kernel. Esta protección debe de poder ser utilizada en agentes Windows, Linux, MacOS.

Si cumple



1.68. Debe estar en capacidad de detener comportamientos considerados como malicioso 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.

Si cumple

1.69. La protección no debe depender de una conexión a la consola de administración.

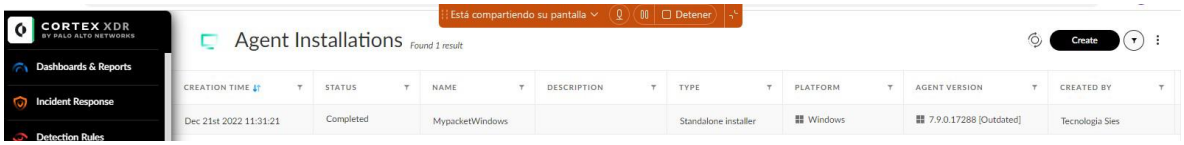
Si cumple

1.70. Debe poder generar hashes de procesos en ejecución y verificación de veredictos en una nube de inteligencia de amenazas.

Si cumple

1.71. Debe estar en capacidad de enviar 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.

Si cumple

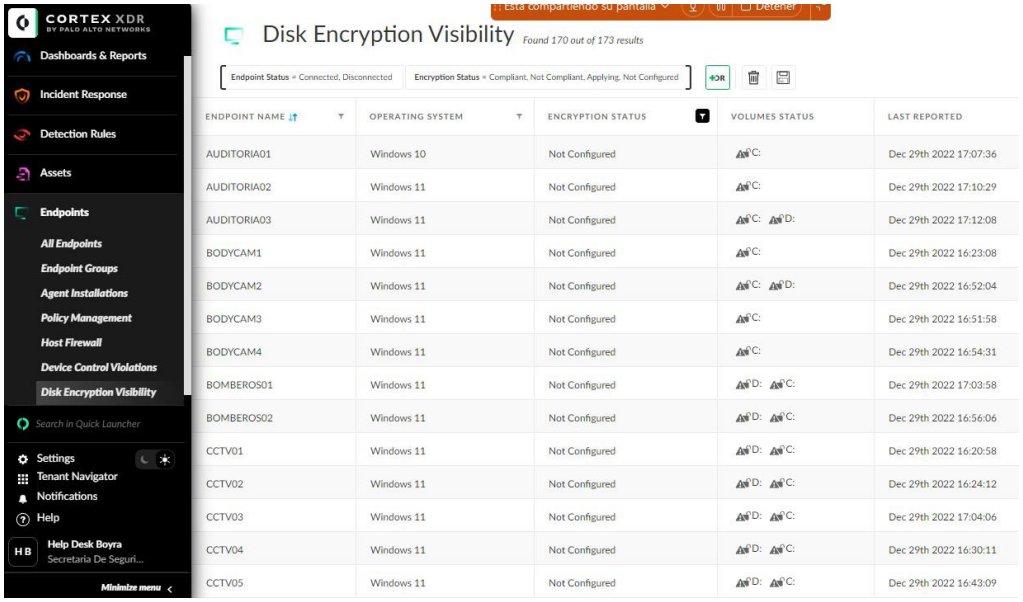


1.72. Debe estar en capacidad de prevenir contra shells reversos (reverse shell) para sistemas operativos Linux.

Si cumple

1.73. Debe estar en capacidad de poder 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.

Si cumple



1.74. 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.

Si cumple

1.75. 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.

Si cumple

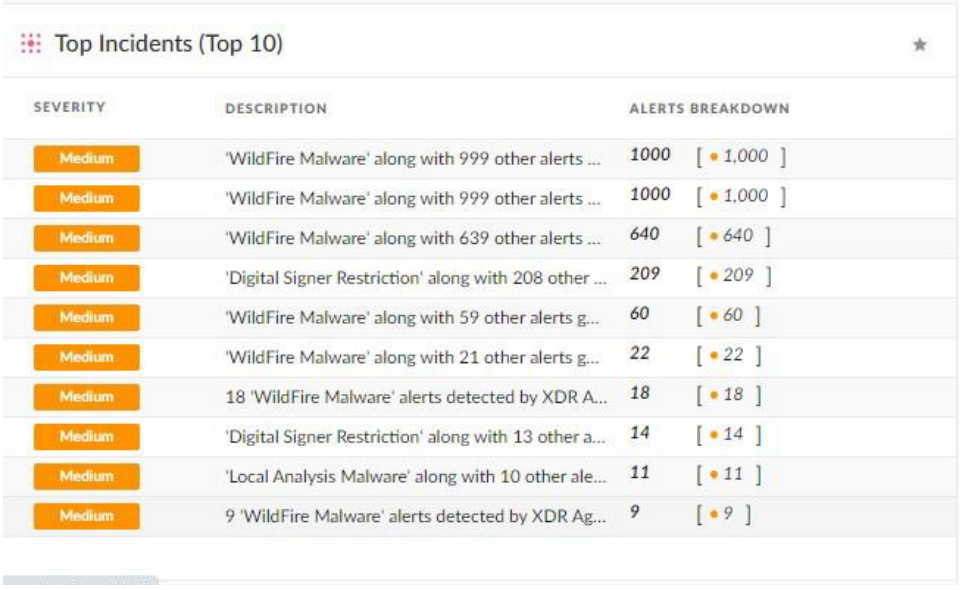


1.76. Debe estar en capacidad para proteger contra ataques de minería de bitcoins para dispositivos Linux, detectados por su comportamiento.

Si cumple

1.77. Debe ser capaz de utilizar 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, Linux, MacOS.

Si cumple



1.78. Debe prevenir la ejecución de procesos utilizando su hash, de manera que el administrador puede determinar qué aplicaciones pueden ser ejecutadas.

Si cumple
1.79. Debe tener 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.

Si cumple

1.80. Debe tener la capacidad de proporcionar protección contra malware sin necesidad de tener una conexión a la consola ni a Internet.

Si cumple

1.81. Debe tener la capacidad de proporcionar protección contra malware sin necesidad de contar con firmas, patrones y/o heurísticas.

Si cumple

1.82. Debe de permitir poner los archivos detectados como maliciosos en una cuarentena, ya sea de manera automática o bajo demanda.

Si cumple

1.83. Debe temer la capacidad de prevenir la ejecución de archivos DMG maliciosos conocidos y examinar en un servicio de análisis en la nube aquellos archivos DMG desconocidos. Si el veredicto de este análisis es malicioso, deberá de bloquear ejecuciones posteriores.

Si cumple

1.84. Debe permitir realizar el escaneo de archivos ejecutables sin la necesidad de firmas.

Si cumple

1.85. Debe permitir programar el escaneo de archivos de manera semanal o mensual.

Si cumple

1.86. Debe permitir definir el día y la hora en la cual se iniciará el escaneo.

Si cumple

1.87. Debe permitir habilitar el escaneo de dispositivos de almacenamiento removible.

Si cumple

1.88. Debe permitir crear listas blancas de carpetas para que sean excluidas del proceso de escaneo.

Si cumple

1.89. Debe permitir poner en cuarentena los archivos identificados como maliciosos, si es que la política está configurada de esta manera.

Si cumple

1.90. El escaneo de archivos deberá de poder analizar los archivos desconocidos de forma estática para determinar si son maliciosos, así como enviar estos archivos desconocidos al servicio de análisis en la nube para que sean analizados.

Si cumple

1.91. Debe estar en capacidad de realizar la administración de políticas centralizado, vía una consola web.

Si cumple

1.92. La consola debe clasificar los eventos en tres niveles de acuerdo a su severidad: bajo, medio y alto.

Si cumple

1.93. La consola de administración debe identificar claramente los eventos que han sido reportados y/o bloqueados y aquellos que han sido detectados.

Si cumple

1.94. Debe estar en capacidad para clasificar el estado de los incidentes en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional.

Si cumple

1.95. Debe estar en capacidad para clasificar el estado de las alertas en cuatro distintos niveles de severidad: alto, mediano, bajo e informacional.

Si cumple

1.96. Debe estar en capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto del mismo.

Si cumple

1.97. Debe estar en capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.

Si cumple

Centro Administrativo Distrital – CAD – Calle 44 No. 52 – 165
Línea Única de Atención a la Ciudadanía 44 44 144
www.medellin.gov.co
Medellín - Colombia

1.98. La consola deberá de proporcionar información detallada bajo demanda de los eventos identificados como exploits.

Si cumple

1.99. Deberá permitir la actualización y desinstalación del agente a partir de la consola.

Si cumple

1.100. Deberá permitir utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.

Si cumple

1.101. Debe contar la capacidad para realizar la integración con Active Directory para la gestión de computadoras y configuración de políticas.

Si cumple

1.102. Debe tener la capacidad de poder crear perfiles granulares.

Si cumple

1.103. Debe contar con la capacidad de poder crear políticas basadas en los perfiles creados.

Si cumple

1.104. Debe tener la capacidad de poder aplicar políticas a usuarios, grupos, computadoras o unidades organizacionales de Active Directory.

Si cumple

1.105. Debe tener la capacidad de crear grupos virtuales que pueden alimentarse de forma estática y dinámica.

Si cumple

1.106. 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.

Si cumple

1.107. La consola deberá de ser proporcionada bajo un esquema software Asa service.

Si cumple

1.108. Debe incluir la capacidad de realizar inspección de datos a nivel de datos de equipos terminales: Creación, eliminación y actualización de archivos, Hash del archivo, Ruta del archivo, Nombre del proceso, Cambio de registro, Argumentos CLI, llamadas RPC e inyección de código, Eventos de hardware, Manipulación de logs de eventos, Alertas de seguridad del agente instalado, análisis de malware.

Si cumple

1.109. Debe contar 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.

Si cumple

1.110. Debe contar 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.

Si cumple

1.111. Debe poder integrarse con una plataforma de ciberseguridad la cual incluya una nube de inteligencia y contextualización de amenazas, a través de un API.

Si cumple

1.112. Debe permitir gestionar las excepciones en una pantalla específica.

Si cumple

1.113. 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 computadoras.

Si cumple

1.114. Deberá de contar con un dashboard en nube que permite visualizar alertas generadas de distintas fuentes.

Si cumple

1.115. Deberá correlacionar alertas, sin importar si estas vengan de datos de endpoint, red o nube y agruparlas dentro de incidentes.

Si cumple

1.116. Deberá de poder mostrar el número total de alertas e incidentes, y debe incluir la capacidad de filtrar la información de forma flexible.

Si cumple

1.117. 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.
Si cumple

1.118. El producto deberá de mostrar información específica de cada proceso involucrado en la secuencia gráfica.

Si cumple

1.119. En la pantalla emergente, en caso de estar disponible, deberá de mostrarse los datos relacionados con el perfil de comportamiento y la ejecución del archivo.

Si cumple

1.120. El producto deberá mostrar una advertencia cuando un ejecutable en particular, que forme parte de la secuencia gráfica, tenga un comportamiento sospechoso.

Si cumple

1.121. 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.

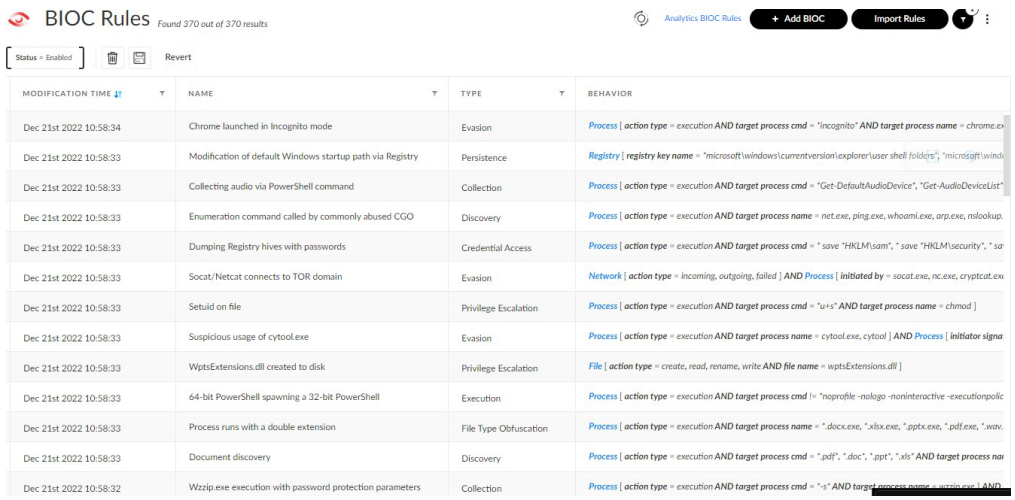
Si cumple

1.122. 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.

Si cumple

1.123. 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.

Si cumple



1.124. El producto deberá de proporcionar la capacidad de decodificar cadenas de caracteres codificadas en base-64 para mostrarlo en texto plano.

Si cumple

1.125. El producto deberá integrarse con los Firewalls de la entidad, recolectando los logs de red que este produzca.

Si cumple

1.126. 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.

Si cumple

1.127. 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.

Si cumple

1.128. 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-

Si cumple

1.129. 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.

Si cumple

1.130. 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.

Si cumple

1.131. El producto deberá proporcionar de manera gráfica la interacción que existe entre uno o varios procesos que sean investigados. La gráfica deber de mostrar la interacción entre los procesos, y si existe una relación entre las computadoras que ejecutan dichos procesos, entre otros aspectos.

Si cumple

1.132. La solución debe haber participado y obtenido un muy buen resultado en los 4 test realizados por MITTRE (Carbanak + Fin 7, APT3, APT 29 y Wizard Spider + Sandworm).

Si cumple

1.133. La solución debe haber obtenido resultados de al menos 74% de detecciones en "Analytic Coverage" para el test APT 29 del 2019 realizado por MITTRE.

Si cumple

1.134. La solución debe haber obtenido resultados de al menos 84% de detecciones en "Analytic Coverage" para el test Carbanak+FIN7 del 2021 realizado por MITTRE.

Si cumple

1.135. La solución debe contar al menos con calificación AA en el último test realizado por CYBERRATINGS para AEP (Advanced Endpoint Protection).

Si cumple

1.136. Debe tener una capacidad de visibilidad de detección del MITTRE
ATT&CK del 100% en protección de amenazas y 97% en visibilidad de detección.

Si cumple

2. CARACTERÍSTICAS DE AGENTE(END POINT)

2.1. Se debe incluir los agentes para al menos 250 dispositivos que se puedan instalar en sistemas operativos Windows, MacOS, Linux sin necesidad de reiniciar.

Si cumple

2.2. Los agentes deben poderse instalar en equipos físicos, máquinas virtuales, en contenedores, en dispositivos móviles, en entornos de nube privada, nube publica, nube hibrida.

Si cumple

2.3. El agente debe tener un footprint mínimo que no impacte la experiencia de usuario.

Si cumple

2.4. Soporte para las siguientes versiones de sistemas operativos: Windows XP* (32-bit, SP3 o posterior), Windows Vista (32-bit, 64-bit, SP1 o posterior; FIPS mode), Windows 7 (32- bit, 64-bit, RTM & SP1; excepto Home), Windows Embedded 7 (Standard & POSReady), Windows 8* (32-bit, 64-bit), 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 2003* (32-bit, SP2 o posterior), Windows Server 2003 R2 (32-bit, SP2 o posterior), Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode), 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. OSX 10.10 (Yosemite), OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14. 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.

Si cumple

2.5. Debe incluir la capacidad de examinar los datos de los equipos terminales que tengan los agentes instalados, las alertas de terceros y los datos de logs.

Si cumple

2.6. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.

Si cumple

2.7. Debe permitir que las VPN client-to-site operen usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.

Si cumple

2.8. Debe soportar para los siguientes ambientes virtuales: VMware ESX, Citrix XenServer, Oracle Virtualbox, Microsoft Hyper-V.

Si cumple
2.9. Debe soportar para máquinas virtuales en nube pública y ambientes de contenedores de servicio como: Google Kubernetes (GKE), Amazon Elastic Kubernetes Service (EKS) y Azure Kubernetes Service (AKS)

Si cumple

2.10. Debe tener la capacidad para configurar la captura de datos que serán enviados a la nube para su almacenamiento, procesamiento y análisis en una consola de detección y respuesta a incidentes.

Si cumple

2.11. Debe incluir la capacidad de realizar inspección de datos a nivel de información del host: Información del Host: Nombre de host, Dirección MAC, Sistema operativo.

Si cumple

2.12. La protección de los equipos terminales (end points) debe incluir la búsqueda y destrucción de amenazas, indexando todos los archivos de los equipos con sistemas operativos Windows, Linux, MacOS que pueda encontrar y eliminar los archivos maliciosos en tiempo real.

Si cumple

2.13. Debe estar en capacidad de evaluar las vulnerabilidades, que le permitan una total visibilidad en tiempo real de la exposición a la vulnerabilidad y los niveles actuales de parches en sus endpoints para priorizar la mitigación.

Si cumple

2.14. El agente de punto final que realice la prevención y recolección de información en el punto final debe ser uno.

Si cumple

3. NGFW (NEXT GENERATION FIREWALL) VIRTUALES SOLICITADOS EN ALTA DISPONIBILIDAD PARA LA SOLUCIÓN XDR

3.1. La solución XDR debe incluir firewall VIRTUALES de nueva generación para instalar en máquinas virtuales tipo VM WARE con la siguiente configuración:

- 4 VCPUS
- 10GB de Memoria RAM1
- 100 GB Disco SSD

Los firewall deben ser de la misma marca que la solución de XDR, para garantizar su interoperabilidad, funcionando en alta disponibilidad. Todas las licencias deben ser por un periodo no inferior a 3 años.

Si cumple

3.2. Los Firewall deben incluir las siguientes funcionalidades: IPS (Intrusion Prevention System) sistema de prevención de intrusiones, control de aplicaciones, filtrado de contenido, antimalware, Antispyware, control de amenazas de día cero, control de archivos, calidad de servicio basado en aplicación y VPN (client-to-site y site-to-site) con validación de postura para dispositivos finales.

Si cumple

3.3. El fabricante debe pertenecer al cuadrante de líderes de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales” en los últimos 6 reportes.

Si cumple

3.4. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.

Si cumple

3.5. Cada Firewall debe soportar:

Al menos 800.000 sesiones
Soportar al menos 9.500 reglas de seguridad
Soportar al menos 40 zonas de seguridad
Debe soportar al menos 1.000 túneles de seguridad VPN IPSEC
Soporte para un tráfico de al menos 2.9Gbps con los siguientes controles activos para todo el tráfico: Control de Apps, DNS security, Sandbox, Control de Archivos, Antimalware, Antiexploit, Anti spyware y logging activo, medido en condiciones reales.

Si cumple

3.6. El equipo debe contar de manera nativa con interfaz gráfica web (GUI) y Línea de comandos (CLI) e Interfaz de programación de aplicaciones (Rest API).

Si cumple

3.7. Debe soportar configuraciones de alta disponibilidad Activo/Pasivo y Activo/Activo con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).

Si cumple

3.8. Debe permitir el control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.

Si cumple

3.9. Debe permitir el agendamiento de las políticas de seguridad.

Si cumple

3.10. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.

Si cumple

3.11. Debe permitir crear o editar políticas de seguridad utilizando el uso de una descripción, tag o comentario de auditoría. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria.

Si cumple

3.12. Debe contar con mecanismos que faciliten la optimización de reglas de seguridad:

a. Mostrar la primera y última vez que se utilizó una regla de seguridad.
b. Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso desde un período definido.

Si cumple

3.13. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.

Si cumple

3.14. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido.

Si cumple

3.15. Debe reconocer mínimo 3000 aplicaciones diferentes, incluyendo: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, audio, vídeo, proxy, mensajería instantánea, email.

Si cumple

3.16. Debe permitir hacer filtros de aplicaciones por comportamiento, popularidad, riesgo, entre otros.

Si cumple

3.17. Debe permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad. Con el objetivo de poder permitir acceder por ejemplo a Office365, Google G Suites para dominio manejados por la organización y no otras cuentas de SaaS dentro de esas nubes.

Si cumple

3.18. Debe identificar aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda.

Si cumple

3.19. La solución de NGFW de seguridad tiene que ser 100% con base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, debe permitir crear 2 políticas.

Si cumple

3.13. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.

Si cumple

3.14. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido.

Si cumple

3.15. Debe reconocer mínimo 3000 aplicaciones diferentes, incluyendo: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, audio, vídeo, proxy, mensajería instantánea, email.

Si cumple

3.16. Debe permitir hacer filtros de aplicaciones por comportamiento, popularidad, riesgo, entre otros.

Si cumple

3.17. Debe permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad. Con el objetivo de poder permitir acceder por ejemplo a Office365, Google G Suites para dominios manejados por la organización y no otras cuentas de SaaS dentro de esas nubes.

Si cumple

3.18. Debe identificar aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda.

Si cumple

3.19. La solución de NGFW de seguridad tiene que ser 100% con base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, debe permitir crear 2 políticas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicación.

Si cumple

3.20. Debe permitir crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las políticas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicación.

Si cumple

3.22. Debe contar con un mecanismo ya sea interno o externo para la optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

Si cumple

3.23. La medida de defensa contra ataques Flood deberán basarse en mecanismos de early drop o random early detection.

Si cumple

3.24. La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Next Generation Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor).

Si cumple

3.25. Debe tener protección contra ataques de escaneo y esta debe permitir definir una lista de excepciones basadas en direcciones IP, a los cuales no se le aplicarán la protección.

Si cumple

3.26. Debe proteger contra ataques basado en paquetes IP, como mínimo: IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route.
Si cumple

3.27. Debe proteger contra ataques basado en paquetes ICMP, como mínimo:
Paquetes con Ping ID 0, paquetes ICMP fragmentados, paquetes ICMP extensos.

Si cumple

3.28. Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2, como Appletalks, Banyan, VINES, Novell, SCADA y otros.

Si cumple

3.29. Debe contar con un mecanismo que proteja contra la saturación del buffer de paquetes por cada interfaz de datos de la solución.

Si cumple

3.30. Debe permitir seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red), Anti-Spyware (o Antibot).

Si cumple

3.31. Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.

Si cumple

3.32. Cuando se utilicen las funciones de IPS, Antivirus y Antispyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Antivirus y Antispyware habilitadas simultáneamente.

Si cumple

3.33. Los firewall virtuales deberán soportar el throughput solicitado, operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware.
Si cumple
3.34. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti- Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.

Si cumple

3.35. Debe combinar un motor de prevención de amenazas en tiempo real con una base de datos URL completa y elementos de identificación de aplicaciones para limitar la transferencia no autorizada de datos y archivos y detectar y bloquear una amplia gama de exploits, malware, navegación web peligrosa y objetivos y amenazas desconocidas.

Si cumple

3.36. La solución debe contar con inspección de archivos ejecutables de Windows, Linux, MacOS en un sandbox (nube o premisas) que pueda recibir mínimo 20 archivos desconocidos por minuto.

Si cumple

3.37. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, e-Directory y base de datos local.

Si cumple

3.38. Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs.

Si cumple

3.39. Debe poseer mínimo 60 categorías de URLs, incluyendo las de malware y phishing.

Si cumple

3.40. Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.
Si cumple
3.41. Debe contar con capacidades técnicas de Inteligencia Artificial localmente o en los laboratorios de inteligencia de amenazas del fabricante de la solución.

Si cumple

3.42. Debe incluir la capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell directory, Exchange y base de datos local.

Si cumple

3.43. Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy, vía Syslog, XFF (X-forwardfor) en la cabecera HTTP y/o XML API, así como la lectura mediante WMI a equipos Windows, Linux, MacOS para la identificación de direcciones IP y usuarios.

Si cumple

3.44. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM u otro protocolo que tenga el mismo fin.

Si cumple

3.45. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.

Si cumple

3.46. Debe permitir la definición de grupos dinámicos de usuarios.

Si cumple

3.47. Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server

Si cumple

3.48. Debe permitir la identificación de los usuarios de la red utilizando una variedad de métodos de acceso y sistemas operativos, incluidos Microsoft Windows, Apple iOS, Mac OS, Android y Linux / UNIX.

Si cumple

3.49. Debe de poder leer las direcciones IPv4 o IPv6 de los usuarios desde el encabezado X-Forwarded-For (XFF) en las solicitudes del cliente HTTP cuando el firewall se implementa entre Internet y un servidor proxy que de otro modo ocultaría las direcciones IP del usuario.

Si cumple

3.50. La solución de NGFW debe tener la capacidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, como: YouTube o Netflix, entre otros por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.

Si cumple

3.51. El QoS (Quality of Service por sus siglas en inglés) debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.

Si cumple

3.52. Debe permitir identificar los archivos por extensión y firmas.

Si cumple

3.53. Debe permite identificar la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.

Si cumple

3.54. Debe soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.

Si cumple

3.55. Debe permitir crear VPN IPSec que soporte como mínimo:
-DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
-Autenticación MD5, SHA-1, SHA-2.
-Diffie-Hellman Group 1, Group 2, Group 5 y Group 14.
-Algoritmo Internet Key Exchange (IKEv1 & IKEv2).

Si cumple

3.56. Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site.

Si cumple

3.57. Debe soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, certificados digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).

Si cumple

3.58. Debe soportar Split Tunel, de tal forma que el tráfico hacia internet no se enrute por la VPN.

Si cumple

3.59. Debe permitir ser administrado por una consola web que pueda trabajar en varios idiomas, como mínimo inglés y español.

Si cumple

3.60. La administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante.

Si cumple

3.61. Debe contar con un dashboard que permita monitorear las sesiones y CPU del equipo Firewall, estado de las interfaces, versión de firmware y última fecha de actualización de la base de datos de las firmas de seguridad.
Si cumple
3.62. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de
Seguridad.

Si cumple

3.63. Debe contar con un dashboard interactivo y gráfico que permita monitorear el tráfico asociado a amenazas de seguridad como malware, spyware, exploits, análisis de malware de día cero, acceso a dominios maliciosos, aplicaciones que no utilizan puerto estándar. Esta información podrá ser filtrada en base a un rango de tiempo, IP, usuario, país y regla de seguridad.

Si cumple

3.64. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino).

Si cumple

3.65. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.

Si cumple

3.66. La solución debe permitir la gestión de dos o más administradores logueados en el Next Generation Firewall, realizando cambios en simultáneo en la consola de gestión y aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.

Si cumple
3.67. El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis en una plataforma de tipo sandbox, la cual podrá ser en versión nube o appliance on- premise.

Si cumple

3.68. El sistema de sandbox deberá contar con certificación de seguridad y privacidad de datos, como mínimo SOC Tipo 2 o FedRAMP.

Si cumple

3.69. La plataforma de Sandboxing deberá tener capacidades robustas para entornos de altos requerimientos de ciberseguridad. Como mínimo se requiere que el Sandbox propuesto

realice la actualización de firmas de nuevos malware detectados en un tiempo no mayor a 24 horas.

Si cumple

3.70. El sistema de Sandbox deberá tener la capacidad de enviar como mínimo 20 archivos desconocidos por minuto para ser analizados. Deberá emular los archivos sospechosos en entornos Windows, Linux, MacOS sin estar limitado a una capacidad de hardware ni Ms (Virtual Machines).

Si cumple

3.71. Debe soportar la inspección de archivos que viajen por los protocolos HTTP, HTTP/2, HTTPS, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Deberá tener cobertura tanto en IPv4 como en IPv6.

Si cumple

3.72. La solución de VPN Avanzada del firewall deberá contar con las siguientes funcionalidades de HIP:
A. Debe permitir la configuración de políticas de seguridad de VPN basado en las características del equipo, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que si el equipo no cumple cierta condición basado en esas características (Perfilamiento y Postura), no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.
B. El Perfilamiento y postura mencionado en el punto anterior, tiene que poder efectuarse inclusive dentro de la red, entre dos o más segmentos de red que controle el firewall, sin necesidad de armar un túnel de VPN, sino solamente utilizando el perfilamiento y postura del equipo de punto final sobre las políticas de seguridad del NGFW.

Si cumple

C. Deberá permitir aplicar el perfilamiento de la maquina dentro de las políticas de seguridad para equipos que estén dentro de la red corporativa (sin requerir túnel VPN) o remotos (Con túneles VPN).

Si cumple

3.80. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
- Tecnología utilizada en las aplicaciones (Client-Server, Browser Based, Network Protocol).

- Nivel de riesgo de las aplicaciones.
- Categoría y sub-categoría de aplicaciones.

Si cumple

3.81. Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las políticas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicación.

Si cumple

3.82. Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

Si cumple

3.83. La protección contra ataques Flood debe permitir definir 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS.
Si cumple
3.84. Debe proteger contra ataques basado en paquetes TCP, como mínimo Split Handshake, paquetes TCP SYN y TCP SYN/ACK con datos contenidos durante el handshake, Validación del Three Handshake.

Si cumple

3.85. Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS.

Si cumple

3.86. Debe permitir como acción ante peticiones DNS maliciosas: alertar, bloquear las conexiones y además responder a la petición con IP sumidero (sinkhole) con el fin de identificar al usuario/equipo realizando consultas DNS maliciosas.

Si cumple

3.87. Debe brindar analítica de cada consulta DNS: frecuencia de visita, marca de tiempo, información del DNS pasiva, WHOIS y cualquier etiqueta de malware asociada.

Si cumple

3.88. El dispositivo debe poder acceder y descargar protecciones contra malware de día 0 en tiempo real.

Si cumple

3.89. Debe emular los archivos sospechosos en entornos Windows, Linux, y Mac sin estar limitado a una capacidad de hardware ni Ms (Virtual Machines).

Si cumple

3.90. Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.

Si cumple

4. ACUERDOS DE NIVELES DE SERVICIO, DISPONIBILIDAD Y CONFIABILIDAD

4.1. ANS Dde acuerdo con la criticidad del problema se define:

Criticidad Alta 1: La red se “cayó” o hay un efecto crítico en sus operaciones de negocios. Se debe tener el soporte 24x7, con un tiempo de respuesta de 2 horas.

La atención puede ser en sitio o remota.

Criticidad Media: La operación de la red existente está afectada, dañada o aspectos significativos de su operación de negocios se ven afectados negativamente por el desempeño inadecuado. Se debe tener el soporte 24x7, con un tiempo de respuesta de 4 horas

Criticidad Baja: El desempeño operativo de la red se ve afectado, mientras que las operaciones de negocios permanecen funcionando. Se debe tener el soporte 8x5, con un tiempo de respuesta del siguiente día hábil.

4.2. La solución completa debe tener una disponibilidad del servicio de mínimo 99.9% contabilizados mensualmente.

4.3. Debe garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, FedRAMP.

4.4. Debe ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.

4.5. El Next Generation Firewall debe ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.

4.6. Deber contar con una acreditación que el servicio se encuentra alineado a los estándares HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) y PCI (Payment Card Industry Data Security Standard. Esta acreditación deberá ser dada por una entidad tercera al fabricante.

4.7. Se debe capacitar al personal técnico en la administración y manejo de la herramienta. Además, se debe prestar servicio de acompañamiento técnico durante los 3 años del soporte y licenciamiento.

4.8. Para todos los equipos y accesorios (hardware y software) del presente proceso el servicio de soporte debe ser por tres (3) años con reemplazo de partes de fábrica 24x7x4 y actualización del software adquirido a través del contratista a la última versión estable liberada por fabricante, para lo cual el oferente deberá adjuntar certificación firmada por el representante legal o quien haga sus veces.

4.9. Para todos los equipos y accesorios (hardware y software) del presente proceso el servicio de soporte debe ser por tres (3) años con reemplazo de partes de fábrica 24x7x4 y actualización del software adquirido a través del contratista a la última versión estable liberada por fabricante, para lo cual el oferente deberá adjuntar certificación firmada por el representante legal o quien haga sus veces.

4.10. Mostrar la primera y última vez que se utilizó una regla de seguridad y mostrar a través de un filtro, las reglas de seguridad que no han tenido uso desde un período definido.

4.11. Los datos de uso de reglas de políticas le permiten validar las adiciones y cambios de reglas y monitorear el período de tiempo cuando se usó una regla. Por ejemplo cuando migra reglas basadas en puertos a reglas basadas en aplicaciones, crea una regla basada en aplicaciones sobre la regla basada en puertos y comprobar si hay tráfico que coincida con la regla basada en puertos. Después de la migración, los datos del conteo de visitas lo ayudan a determinar si es seguro eliminar la regla basada en el puerto al confirmar si el tráfico coincide con la regla basada en la aplicación en lugar de la regla basada en el puerto.

4.12. El conteo de aciertos de la regla de política lo ayuda a determinar si una regla es efectiva para la aplicación de acceso. ¨

El contratista deberá cumplir con los protocolos de bioseguridad y la dotación de los elementos de protección personal de acuerdo a la normativa vigente y con el fin de contribuir a prevenir el contagio del COVID-19. El supervisor deberá dejar constancia de la verificación de este requisito.

El Supervisor y/o Interventor, deberá dejar evidenciado el cumplimiento de las obligaciones a cargo del contratista en materia de impuestos y contribuciones aplicables al respectivo contrato. Para ello extraerá del Sistema de Seguimiento a la contratación SAP transacción "ZMMPUR179 - Reporte Retenciones por Contrato", el siguiente cuadro como ejemplo, anotando que la "Descripción del indicador" varía según cada contrato:

Descripción Indicador	Valor Retención
Estampilla bienestar Adulto Mayor	
Estampilla Pro Cultura de Medellín 0,5%	
Estampilla Universidad de Antioquia	
Ret.impto.renta compra bienes Gener 2.5	
Retención ICA 2*1000 art 54 Acuer 64/12	
Retención IVA 15% Ley. 1607 de 2012	
Tasa Prodeporte Y Recreacion 1.3%	
Total general	

INFORME ADMINISTRATIVO:

- El contratista se encuentra al día en el pago de las obligaciones frente al Sistema Integral de Seguridad Social y Parafiscales, según certificación que se detalla a continuación:

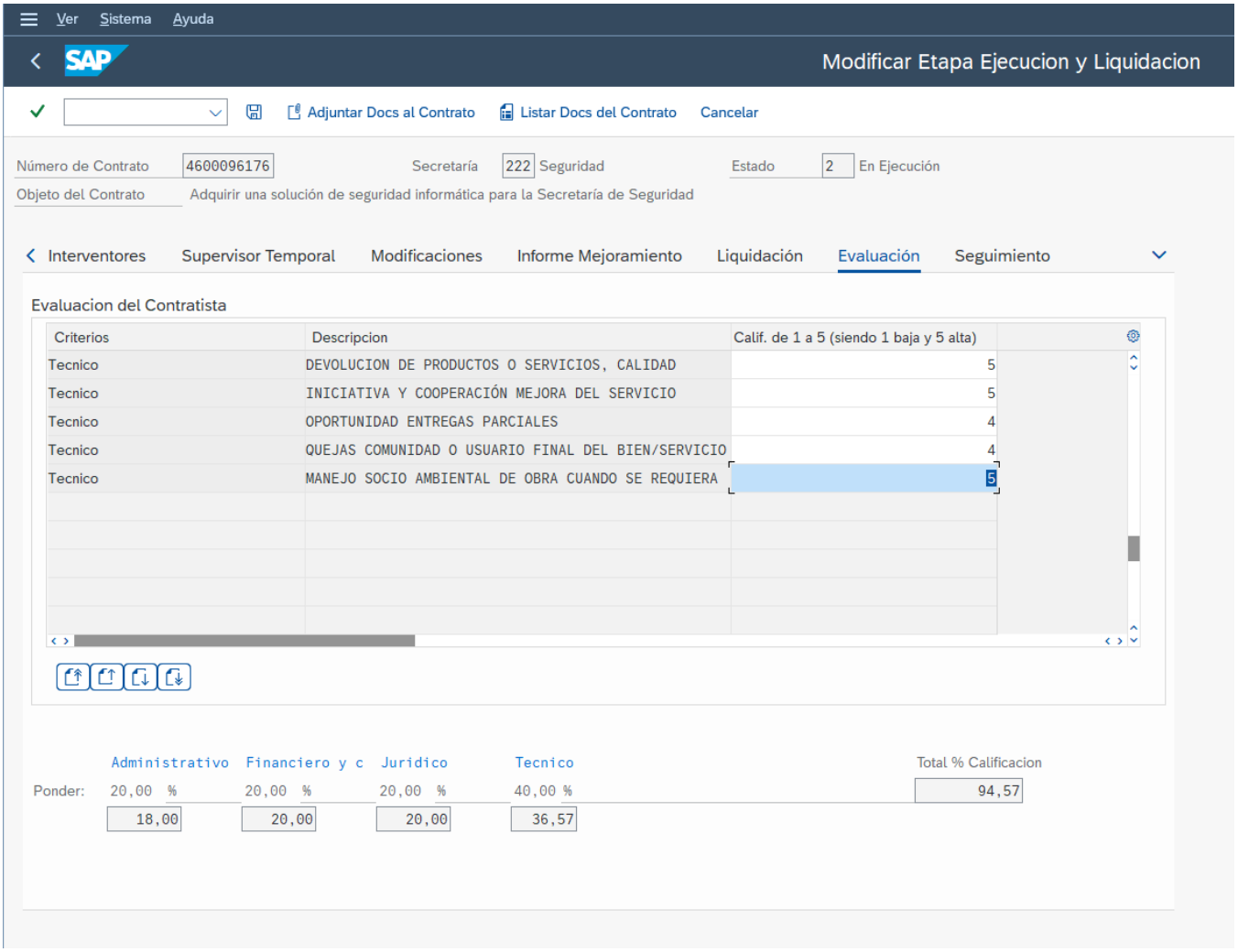
Fecha del Documento	Fechas de cobertura de la certificación del pago realizado al Sistema de	Relación de los datos de quien firma el documento (Firmado por el Revisor Fiscal o

	Seguridad Social Integral	Representante Legal)
27/12/2022	De Julio a 31 de diciembre de 2022	FABIO HUMBERTO OSPINA MIRANDA C.C. 88.196.034 expedida en Cúcuta Tarjeta Profesional 74624 – T Revisor Fiscal de BOYRA S.A.

- No aplica para este contrato la subcontratación autorizada por el Distrito.
- No aplica registro ni marcación de bienes.
- No se han realizado modificaciones al contrato.
- Se realizó la siguiente designación de supervisión unipersonal con apoyos:

Fecha	Supervisor	Apoyo Técnico	Apoyo Jurídico	Apoyo Administrativo, financiero y contable	Supervisor suplente
13/12/2022	Andrés Felipe García Foronda	Horacio Grisales Noreña	Mario Fabián Bucheli Naranjo	Vanessa Suárez González	Nereida Hernández Coronado

- No se han materializado riesgos en el contrato.
- No aplica contratos de comodato.
- Evaluación al contratista en SAP.



- El contrato no ha sido auditado por los entes de control ni por la Secretaría de Evaluación y Control.

5. INFORME FINANCIERO Y CONTABLE:

- Relación de la imputación del gasto:

Fondos	Centro Gestor	Posición Presupuestal (Pospre)	Proyecto	CDP	Solicitud de Pedido (Solpedido)	Registro Presupuestal (Pedido)
110701720	73200000	2320202008	200272	4000111033	9014703	4500014221

Centro Administrativo Distrital – CAD – Calle 44 No. 52 – 165
Línea Única de Atención a la Ciudadanía 44 44 144
www.medellin.gov.co
Medellín - Colombia

- Se realizó justificación de saldo a 31 de diciembre de 2022 en el pedido 4500014221 por valor de 1.107.000.000, teniendo en cuenta la duración y forma de pago del contrato.

- No se han realizado pagos

- Informe de ejecución financiera del contrato por proyectos:

Contrato	Registro Presupuestal (Pedido)	Grupo de compras	Denominación Grupo de Compras	Proyecto	Nombre Proyecto	Valor proyecto por pedido	Valor Facturado por proyecto del pedido	Saldo por proyecto del pedido
4600096176	4500014221	222	Seguridad	200272	FORMULACIÓN E IMPLEMENTACIÓN DEL PLAN ESTRATÉGICO EN TECNOLOGÍA DE INFORMACIÓN Y TELECOMUNICACIONES PARA LA SEGURIDAD Y LA CONVIVENCIA	1.107.000.000	0	1.107.000.000

- Resumen de la ejecución de los recursos:

Valor del contrato	1.107.000.000
Adiciones	0
Total valor del contrato más adiciones	1.107.000.000
Pagos realizados (acumulado)	0
Pago autorizado del periodo	1.107.000.000*
Porcentaje de ejecución financiera	0%

Centro Administrativo Distrital – CAD – Calle 44 No. 52 – 165
Línea Única de Atención a la Ciudadanía 44 44 144
www.medellin.gov.co
Medellín - Colombia

*Como el pago no se alcanzó a realizar antes del cierre de facturación del Distrito de Medellín en la vigencia 2022, se autoriza el pago por valor de mil ciento siete millones de pesos M.L ($1.107.000.000) IVA incluido, una vez se expida la resolución de ajustes y reservas y se realicen a nivel interno las actualizaciones de fichas y los traslados presupuestales correspondientes. Lo anterior de conformidad con la forma de pago establecida.

INFORME JURÍDICO:

- De conformidad con el artículo 86 de la Ley 1474 de 2011, no se presentaron reclamaciones, controversias y acuerdos entre las partes, y en ese orden de ideas no se adelantó ningún tipo de actuación administrativa de carácter sancionatorio, en relación con incumplimientos, multas, cláusula penal o declaración de la caducidad.

- En observancia de los artículos 8° y 9° de la Ley 80 de 1993, concordados con los artículos 1° y 90 de la Ley 1474 de 2011, se tiene que el contratista no fue sujeto de sanción penal, disciplinaria, fiscal o correctiva, así como acumulación de multas y sanciones que limiten su capacidad para ejecutar y liquidar bilateralmente el contrato objeto de supervisión, por lo tanto no estuvo incurso en ninguna causal de inhabilidad sobreviniente.

- Estado de las garantías del contrato: En la celebración del presente contrato, quedaron establecidas las garantías de común acuerdo entre las partes, las cuales fueron expedidas por el contratista y aprobadas por la entidad de la siguiente:

Nombre Aseguradora	N° Póliza	Tipo de Amparo	Cobertura de la Póliza		Fecha de Aprobación de la Garantía	Valor Amparado
			Desde	Hasta		
SEGUROS DEL ESTADO S.A	**14-44-101169543**	Cumplimiento del contrato	09/12/2022	30/06/2023	12/12/2022	$110.700.000
		Calidad del servicio	09/12/2022	31/12/2023	12/12/2022	$110.700.000

- El apoyo jurídico a la supervisión del presente contrato estima que de conformidad con los preceptos establecidos en la Ley 80 de 1993, Ley 1150 de 2007 en lo pertinentes a la supervisión de los contratos estatales, Ley 1474 de 2011 y demás normas que regulan la materia, no se evidencia situación de orden que pueda afectar la ejecución del objeto contractual.

- Se realizó la publicación en el sistema electrónico para la contratación pública SECOP II, dando cumplimiento a los requisitos legales y al principio de publicidad establecido en el Decreto 1082/2015.- Artículo 2.2.1.1.1.7.1.

Atentamente,

ANDRÉS FELIPE GARCÍA FORONDA
Supervisor

Apoyos a la supervisión:

- **Horacio Grisales Noreña** - Apoyo Técnico
- **Mario Fabián Bucheli Naranjo -** Apoyo Jurídico
- **Vanessa Suárez González** - Apoyo Administrativo, Financiero y Contable

Centro Administrativo Distrital – CAD – Calle 44 No. 52 – 165
Línea Única de Atención a la Ciudadanía 44 44 144
www.medellin.gov.co
Medellín - Colombia