Página 1 de 14 Código: 2BS-FR-0019	ELABORACIÓN, EJECUCIÓN Y LIQUIDACIÓN DE CONTRATOS	POLICÍA NACIONAL
Fecha: 12-03-2021 Versión: 5	INFORME DE SUPERVISIÓN DE CONTRATOS U ÓRDENES DE COMPRA	

Nro. 058445 **DICAR-SIPOL**

Bogotá D.C.; 4 de diciembre de 2023

Señor coronel
WILLIAM CASTAÑO RAMOS
Director de Carabineros y Protección Ambiental
Bogotá D.C.

ASUNTO: informe de supervisión Contrato de compraventa 71-2-10038-23

TIPO DE INFORME

PERIÓDICO X **FINAL** ___

Periodo del informe de supervisión

Desde	**27/10/2023**	**Hasta**	**30/11/2023**

En cumplimiento a los artículos 83 y 84 de la Ley 1474 de 2011 "*Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública*", así como de la Resolución No.03049 del 30 de julio del 2014 "*Por la cual se adopta el Manual de Contratación de la Policía Nacional*", Resolución No. 00090 del 15/01/2018, "*Por la cual se actualiza, modifica y complementa el Manual de Contratación de la Policía Nacional adoptado mediante Resolución No. 03049 de 2014*", y la *"Guía para el ejercicio de las funciones de Supervisión e Interventoría de los contratos del Estado*" expedida por Colombia Compra Eficiente, o las normas que las modifiquen, adicionen o sustituyan, sin perjuicio de las funciones establecidas contractualmente y aquellas inherentes a la naturaleza del ejercicio de la supervisión, me permito presentar el correspondiente informe del contrato u orden de compra del asunto a través del cual se detalla, el seguimiento y el grado de cumplimiento de las obligaciones establecidas en el respectivo contrato u orden, así:

INFORMACIÓN GENERAL:

Mediante comunicado oficial GS-2023-051636-DICAR de fecha 26/10/2023, se notifica al señor CAPITÁN FABIAN ESTEBAN MONTAÑA SARMIENTO Jefe de operaciones de la Seccional de Inteligencia Policial DICAR como supervisor de la Contrato de compraventa 71-2-10038-23 cuyo objeto es la "ADQUISICIÓN, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN DISPOSITIVO TIPO FIREWALL PARA LA SECCIONAL DE INTELIGENCIA POLICIAL DE LA DIRECCIÓN DE CARABINEROS Y PROTECCIÓN AMBIENTAL".

- **Periodicidad establecida para la entrega del informe de supervisión:** Mensual
- **No. de informes de supervisión presentados y publicados en SECOP II:** 0

Información del contrato

Contrato No.	Contrato de compraventa 71-2-10038-23
Objeto del Contrato	ADQUISICIÓN, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN DISPOSITIVO TIPO FIREWALL PARA LA SECCIONAL DE INTELIGENCIA POLICIAL DE LA DIRECCIÓN DE CARABINEROS Y PROTECCIÓN AMBIENTAL.
Contratista	BOYRA S.A
Representante legal	LUIS JOSE IGNACIO QUINTERO CUSGUEN
Valor inicial del contrato	CINCUENTA MILLONES PESOS ($ 50.000.000,00), MONEDA CORRIENTE, INCLUIDO I.V.A.
Valor total del contrato	TREINTA Y CUATRO MILLONES SEISCIENTOS MIL PESOS ($ 34.600.000,00), MONEDA CORRIENTE, INCLUIDO I.V.A.
Plazo de ejecución inicial	Del 27/10/2023 al 25/12/2023
Fecha de inicio del plazo de ejecución del contrato	27 de octubre de 2023
Fecha de terminación del plazo de ejecución del contrato	25 de diciembre de 2023
Modificatorios	No aplica
Prorrogas	No aplica
Otros	No aplica

1. DESARROLLO DE LA SUPERVISIÓN AL CONTRATO U ORDEN DE COMPRA

1.1 Acciones adelantadas:

Durante el mes de noviembre se ha realizado 5 llamadas por parte del supervisor del contrato Capitán Fabian Esteban Montaña Sarmiento al representante legal de la empresa contratista BOYRA señor Luis José Ignacio Quintero al abonado celular 3158625709, con el fin de conocer los tiempos y proceso de entrega del FIREWALL.

El día 28/11/2023 se realizó reunión dejando como soporte acta 196 SIPOL – GROPI 2.21 por parte del supervisor del contrato Capitán Fabian Esteban Montaña Sarmiento, donde el representante legal de la empresa contratista BOYRA indica que la empresa fabricante del firewall "Paloalto" la cual se encuentra ubicada en Estados Unidos, no podrá entregar el elemento antes de 26 de diciembre del año en curso. Asimismo, se le indicó al contratista que el presente contrato tiene plazo de 60 días que finalizan el 25 de diciembre 2023, lo cual supondría que estaría fuera de la ejecución contractual.

De la misma manera manifestó, radicar en el sistema SECOP II la solicitud de prórroga teniendo en cuenta los problemas informados por el fabricante para la entrega del elemento.

2. VERIFICACIÓN DEL CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES

CUMPLIMIENTO OBLIGACIONES LEGALES DEL CONTRATISTA

OBLIGACIONES DEL CONTRATISTA LEGALES	CUMPLIÓ	OBSERVACIONES
1. Cumplir con el objeto contractual.	N/A	N/A
2. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y trabas.	N/A	N/A
3. Responder en los plazos que la POLICÍA NACIONAL – DIRECCIÓN DE CARABINEROS Y SEGURIDAD RURAL establezca en cada caso, los requerimientos de aclaración o de información que le formule.	N/A	N/A
4. Cumplir cabalmente con sus obligaciones, frente al Sistema de Seguridad Social Integral y parafiscales (Cajas de Compensación Familiar, Sena e ICBF), por cuanto el cumplimiento de esta obligación es requisito indispensable para la realización de cualquier pago.	N/A	N/A
5. Guardar la confidencialidad de toda la información que le sea entregada y que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o manipular y responderá civil, penal y disciplinariamente por los perjuicios de su divulgación y/o utilización indebida que por sí o por un tercero se cause a la administración o a terceros.	N/A	N/A
6. No acceder a peticiones o amenazas, de quienes actuando por fuera de la ley pretendan obligarlo a hacer u omitir algún acto o hecho, el CONTRATISTA deberá Informar de tal evento a la POLICÍA NACIONAL – DIRECCIÓN DE CARABINEROS Y SEGURIDAD RURAL y a las autoridades competentes para que se adopte las medidas necesarias.	N/A	N/A
7. Mantener activa la cuenta corriente o de ahorros reportada para los pagos con el fin de evitar traumatismos en el proceso de ejecución del contrato.	N/A	N/A

8. Restituir a la POLICÍA NACIONAL – DIRECCIÓN DE CARABINEROS Y SEGURIDAD RURAL los elementos que haya colocado a su disposición para el desarrollo del objeto contractual, cuando se lo requiera o al finalizar el contrato, en caso de que se hayan suministrado.	N/A	N/A
9. CATALOGACIÓN. - EL CONTRATISTA deberá proporcionar la información necesaria para denominar, clasificar, identificar y numerar los artículos de abastecimiento relacionados y/o incluidos en el objeto del contrato, dentro del plazo y en las condiciones señaladas por el Supervisor, quien acreditará el cumplimiento de la presente cláusula, mediante un certificado en que conste la entrega total de la información requerida. La presente certificación será necesaria para la liquidación del contrato. Entendiéndose no finalizada la entrega de los bienes objeto del contrato, en tanto no se cumplan las obligaciones de la cláusula de catalogación.	N/A	N/A
10. Incluir todas aquellas obligaciones que el contratista debe cumplir con el fin de alinear la actividad contractual a las buenas prácticas en materia ambiental. Tener además en cuenta lo establecido en la resolución 03049 del 2014, "Por medio del cual se adopta el Manual de Contratación de la Policía Nacional", actualizada, modificada y complementada por las Resoluciones Nos. 00090 del 2018 apéndice 1 y apéndice 2 del 2020.	N/A	N/A
11. Así mismo incluir las obligaciones en materia de Seguridad y Salud en el Trabajo y los lineamientos del gobierno nacional en el tema del COVID.	N/A	N/A
12. Para la facturación de los bienes o servicios contratados, se debe tener en cuenta los lineamientos y parámetros contemplados en la circular externa 016 del 09 de marzo de 2021 establecidos por el Ministerio de Hacienda y Crédito Público, por medio del cual se implementa el modelo de recepción de facturas de venta, notas débito y/o notas crédito, la cual es de obligatorio cumplimiento, de acuerdo con la Directiva Presidencial 09 del 17 de septiembre de 2020 "Lineamientos para el Pago de Proveedores del Estado" y la Resolución No. 000042 del 05 de mayo de 2020, "Por la cual se desarrollan los sistemas de facturación, los proveedores tecnológicos" y el registro de la factura electrónica de venta.	N/A	N/A

13. Las demás obligaciones del CONTRATISTA contenidas en el artículo 5º de la Ley 80 de 1993, así mismo, será civil y penalmente responsable por sus acciones u omisiones en la actuación contractual.	N/A	N/A

CUMPLIMIENTO ESPECIFICACIONES TÉCNICAS

ITEM	CONDICIONES TECNICAS MINIMAS	CUMPLE	NO CUMPLE
1.	Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial. Cantidad:1 Marca: A establecer por parte de los oferentes Serie: A establecer por parte de los oferentes Cada uno de ellos con las siguientes características	N/A	N/A
1.1	Cada equipo debe venir con el licenciamiento que permita tener características de IPS, control de aplicaciones, filtrado de contenido, antimalware y VPN (client-to-site y site-to-side) con validación de postura para dispositivos finales.	N/A	N/A
1.2	El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en al menos uno de los 3 últimos reportes.	N/A	N/A
1.3	La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.	N/A	N/A
1.4	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.	N/A	N/A
	Los equipos deben soportar protocolo IPv6 para su administración, configuración de políticas, y demás funcionalidades propias de la herramienta a ofertar.	N/A	N/A
1.5	CAPACIDAD		
1.5.1	Throughput de Next Generation Firewall de mínimo 1 Gbps (mediciones hechas con mínimo control de aplicaciones activado)	N/A	N/A
1.5.2	Throughput de Threat Prevention de 690 Mbps mediciones con mínimo las siguientes funcionalidades habilitadas simultáneamente: Firewall con control de aplicaciones, Sistema de Prevención de Intrusos (IPS) y Anti-malware.	N/A	N/A
1.5.3	No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.	N/A	N/A
1.5.4	Debe soportar mínimo 64.000 sesiones simultaneas	N/A	N/A
1.5.5	Debe soportar mínimo 12.000 nuevas sesiones por segundo	N/A	N/A
1.5.6	Disco interno de 128 GB	N/A	N/A
1.5.7	Mínimo 8 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red	N/A	N/A
1.5.8	1 (una) interfaz de red tipo RJ45 de 1 Gbps que se pueda destinar para administración	N/A	N/A
1.5.9	1 (una) interfaz de tipo consola	N/A	N/A
1.5.10	1 Puerto USB	N/A	N/A
1.5.11	Capacidad mínima de 3 instancias de routing virtuales	N/A	N/A
1.5.12	Capacidad mínima de 25 zonas de seguridad	N/A	N/A
1.5.13	El equipo debe contar de manera nativa con interfaz gráfica web (GUI), Línea de comandos (CLI).	N/A	N/A
1.6	CARACTERÍSTICAS GENERALES		
1.6.1	El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, sub-interfaces ethernet lógicas, NAT de origen y destino.	N/A	N/A
1.6.2	Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).	N/A	N/A
1.6.3	Soportar funcionalidades en IPv6	N/A	N/A
1.6.4	Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.	N/A	N/A
1.6.5	Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.	N/A	N/A

1.6.6	Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.	N/A	N/A
1.6.7	Debe permitir el bloqueo de ataques de Denegación de Servicio (DoS).	N/A	N/A
1.6.8	Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer.	N/A	N/A
1.7	**FUNCIONALIDADES DE FIREWALL**		
1.7.1	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 y categorías de aplicaciones.	N/A	N/A
1.7.2	Permitir el agendamiento de las políticas de seguridad.	N/A	N/A
1.7.3	Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.	N/A	N/A
1.7.4	Permitir añadir un comentario de auditoria cada vez que se haga un cambio o se edite la política de seguridad.	N/A	N/A
1.7.5	Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).	N/A	N/A
1.7.6	Debe contar con mecanismos que faciliten la optimización de reglas de seguridad: - Mostrar la primera y última vez que se utilizó una regla de seguridad. - Mostrar a través de un filtro, las reglas de seguridad que no han tenido uso desde un período definido.	N/A	N/A
1.8	**DESCIFRADO DE TRÁFICO SSL/TLS**		
1.8.1	Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.	N/A	N/A
1.8.2	Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.	N/A	N/A
1.8.3	Debe permitir los algoritmos de cifrado para negociar la conexión SSL/TLS, deberá soportar como mínimo los siguientes: RSA, DHE, ECDHE, 3DES, AES-128-GCM, AES-128-CBC, AES-256-GCM, AES-256-CBC, CHACHA20-POLY1305, MD5, SHA1, SHA256, SHA384.	N/A	N/A
1.8.4	Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido	N/A	N/A
1.8.5	Debe poder bloquear las sesiones cuyo certificado no es válido o el emisor no es confiable a pesar de no aplicar descifrado al tráfico SSL/TLS	N/A	N/A
1.8.6	Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.	N/A	N/A
1.8.7	Debe permitir reenviar el tráfico descifrado por una interfaz Port Mirror o Snnifer a un equipo externo al Firewall, como por ejemplo un DLP.	N/A	N/A
1.8.8	Capacidad de poder hacer decifrado a por lo menos TLS v1.1, v1.2 y v1.3	N/A	N/A
1.8.9	La solución tiene que contar con un dashboard de reportes y logs.	N/A	N/A
1.9	**IDENTIFICACION Y CONTROL DE APLICACIONES**		
1.9.1	Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.	N/A	N/A
1.9.2	Las políticas de seguridad tienen que poder ser creadas en base a las aplicaciones y no en base a puertos TCP/UDP.	N/A	N/A
1.9.3	La aplicación de seguridad tiene que ser 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto de comunicaciones, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicación.	N/A	N/A
1.10	**PREVENCION DE AMENAZAS**		
1.10.1	Se debe incluir, para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus (Antimalware de red).	N/A	N/A
1.10.2	Las funcionalidades de IPS y Antivirus 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.	N/A	N/A
1.10.3	Cuando se utilicen las funciones de IPS y Antivirus, el equipamiento debe entregar el mismo performance (no degradar).	N/A	N/A
1.10.4	El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS y Antivirus.	N/A	N/A
1.10.5	Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes.	N/A	N/A
1.10.6	Debe soportar granularidad en las políticas de IPS y Antivirus, 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.	N/A	N/A

1.10.7	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, HTTPS, FTP, SMB (versiones 1,2 y 3), SMTP, IMAP y POP3. Deberá tener cobertura tanto en IPv4 como en IPv6 para los protocolos en mención.	N/A	N/A
1.10.8	Previene ataques utilizando Inteligencia de amenazas global.	N/A	N/A
1.10.9	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.	N/A	N/A
1.10.10	Debe proteger la red de amenazas comunes y amenazas persistentes avanzadas (APT)	N/A	N/A
1.11	**IDENTIFICACION DE USUARIOS**		
1.11.1	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, Exchange y base de datos local.	N/A	N/A
1.11.2	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.	N/A	N/A
1.11.3	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x, soluciones NAC, soluciones proxy por envíos directos y/o vía alguno de los siguientes mecanismos: "RADIUS, Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API".	N/A	N/A
1.11.4	Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.	N/A	N/A
1.11.5	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.	N/A	N/A
1.11.6	Debe permitir la definición de grupos dinámicos de usuarios.	N/A	N/A
1.11.7	Debe de 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.	N/A	N/A
1.12	**CALIDAD DE SERVICIO (QOS)**		
1.12.1	Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix por ejemplo), se requiere que la solución tenga la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.	N/A	N/A
1.12.2	Soportar la creación de políticas de QoS por: dirección de origen y destino, por usuario y grupo de LDAP/AD, por aplicaciones, por puerto.	N/A	N/A
1.12.3	El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.	N/A	N/A
1.13	**FILTRO DE DATOS**		
1.13.1	Los archivos deben ser identificados por extensión y firmas.	N/A	N/A
1.13.2	Permite identificar y opcionalmente prevenir 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.	N/A	N/A
1.14	**VPN**		
1.14.1	Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.	N/A	N/A
1.14.2	La VPN IPSec debe soportar como mínimo:	N/A	N/A
1.14.3	- DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)	N/A	N/A
1.14.4	- Autenticación MD5, SHA-1, SHA-2;	N/A	N/A
1.14.5	- Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;	N/A	N/A
1.14.6	- Algoritmo Internet Key Exchange (IKEv1 & IKEv2);	N/A	N/A
1.14.7	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.	N/A	N/A
1.14.8	Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.	N/A	N/A
1.14.9	Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site.	N/A	N/A
1.14.10	Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).	N/A	N/A
1.14.11	Debe permitir configurar Split Tunel inteligente, que permita seleccionar el tráfico a enrutar en base a la aplicación y dominio de internet. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.	N/A	N/A
1.14.12	Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:	N/A	N/A

1.14.13	- Antes del usuario se autentique en la estación;	N/A	N/A
1.14.14	- Después de la autenticación del usuario en la estación usando Single Sign On (SSO);	N/A	N/A
1.14.15	- Bajo demanda del usuario;	N/A	N/A
1.14.16	Debe asignar una IP a cada cliente que se conecte a la VPN en formato IPv4 e IPv6, de forma automática mediante un pool de IP.	N/A	N/A
1.14.17	El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.	N/A	N/A
1.15	VPN AVANZADA		
1.15.1	El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y ios.	N/A	N/A
1.15.2	La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada.	N/A	N/A
1.15.3	Debe ser posible colocar equipos en cuarentena de forma manual o automática.	N/A	N/A
1.15.4	Debe ser posible bloquear el acceso a red de los equipos colocados en cuarentena.	N/A	N/A
1.15.5	La solución de VPN Avanzada deberá contar con las siguientes funcionalidades de HIP, para al menos 300 usuarios concurrentes: - 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. - 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. - 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). - Debe permitir el aislamiento o cuarentena de una máquina que presente algún indicador de compromiso dentro del tráfico.	N/A	N/A
2	GENERALIDADES		
2.1	Los equipos deberán tener soporte vigente de fábrica durante la ejecución del contrato y por el término de garantía (cinco años), el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware. Así mismo, el soporte del fabricante deberá brindar herramientas de evaluación de configuraciones de los equipos alineadas a las buenas prácticas de la industria y propuestas por el fabricante.	N/A	N/A
2.2	Para todos los equipos y accesorios (hardware y software) del presente proceso el servicio de soporte por garantía debe ser por cinco (5) años con reemplazo de partes de fábrica 24x7 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.	N/A	N/A
2.3	El firewall se deberá entregar en las instalaciones del Almacén del Grupo de las Tecnologías de la Información y las Comunicaciones de la Dirección de Carabineros y Protección Ambiental DICAR, ubicado en la Avenida Boyacá N° 142A-55 Barrio Colina Campestre (Bogotá D.C.), siendo configurado en la Seccional de Inteligencia Policial DICAR	N/A	N/A
2.4	El contratista durante todo el tiempo de instalación, soporte y garantía (cinco años), deberá atender de forma presencial en la Seccional de Inteligencia Policial DICAR con un esquema 24 x 7 en un tiempo máximo de cuatro horas después de reportado el incidente, falla técnica y /o requerimiento de configuración, todas las solicitudes de la entidad generando para esto un numero de incidente al cual se le debe poder realizar la trazabilidad correspondiente.	N/A	N/A
2.5	I soporte técnico debe incluir: • Actualizaciones de programas, parches, reparaciones, parches de seguridad y alertas de seguridad para software de sistema operacional y software integrado. • Soporte de hardware en sitio. • Asistencia 7x24x365 7 días a la semana. • Acceso al (sistema de soporte al cliente sobre plataforma web 24x7) incluyendo la posibilidad de realizar solicitudes de servicio en línea. • El contratista debe recomendar procedimientos operacionales que mitiguen los riesgos de fallas del sistema, además de entregar la documentación, diagrama lógico, usuarios, contraseñas usadas durante las fases de implementación.	N/A	N/A

	Principales versiones de producto y tecnología para software de sistema operacional y software integrado (ej: firmware), que incluye versiones de mantenimiento general, versiones de funcionalidad especifica.		
2.6	El contratista deberá poner a disposición de la Policía Nacional, de manera permanente, los siguientes medios para el reporte de caso: - Mesa de servicio o autoservicio con acceso vía web. - Número Telefónico. - Correo Electrónico. **Tiempo de respuesta** Para la totalidad de los elementos ofertados, se debe brindar soporte técnico telefónico o remoto generado un ticket o número de caso de forma inmediata. El tiempo de respuesta será de 4 horas contadas a partir de la generación del caso o ticket. Si después de haber atendido el incidente y se determine el requerimiento de asistencia en sitio, se enviará personal técnico en un tiempo máximo de 6 horas. El tiempo máximo para restablecer el servicio será de 48 horas	N/A	N/A
2.7	Durante el tiempo de garantía (cinco años), el contratista deberá realizar un mantenimiento preventivo anual en el presente contrato; el cual abarque revisión y ajuste de configuración, actualizaciones, puesta en funcionamiento de nuevas características, aplicación de buenas prácticas, entre otros. El mantenimiento debe incluir: • Verificación de equipos, componentes, revisión de logs, versiones de parches. • Actualizaciones recomendadas por parte del fabricante • Revisión y solución de errores, revisión programación de copias de respaldo. • Reemplazo de partes defectuosas de fábrica siempre y cuando estén dentro de la garantía. • En caso de que la reparación del equipo demore más de setenta y dos (72) horas, el proveedor deberá suministrar en forma inmediata un equipo de soporte de iguales o superiores características durante el tiempo que dure la reparación.	N/A	N/A
2.8	Todas las licencias que requieran los equipos para su funcionamiento deben quedar activas por un término de cinco años, suministrando los documentos de fabricante que las avale.	N/A	N/A
2.9	Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos de soporte.	N/A	N/A
2.10	El servicio deberá incluir al menos una evaluación de buenas prácticas de implementación, la cual deberá ser dirigida por un personal /empleado propio del fabricante de la solución NGFW. Esta evaluación deberá validar el nivel de adopción de buenas prácticas de configuración del NGFW implementado en la Entidad; se deberá entregar un informe con las recomendaciones técnicas para mejorar la configuración del equipo NGFW. Esta evaluación se deberá realizar dentro de los 12 primeros meses posteriores a la implementación del NGFW y previa coordinación con el supervisor del contrato.	N/A	N/A
2.11	Se debe realizar antes de la instalación de los equipos, las validaciones eléctricas, pruebas de carga, mediciones de voltaje, teniendo en cuenta que de ser necesario se debe ejecutar el reemplazo de circuitos, interruptores, traslados entre otros por parte del contratista, sin costo adicional para el contratante.	N/A	N/A
2.12	El contratista deberá entregar todos los cables de poder, patch cord cobre, patch cord de fibra (de acuerdo al tipo de cableado instalado en la Secccional de Inteligencia Policial DICAR), marcados en cada uno de sus extremos de acuerdo a la organización establecida en el centro de cómputo de la unidad.	N/A	N/A
2.13	Se debe organizar el cableado de los lugares donde se instalarán los equipos adquiridos en el presente contrato (incluyendo peinado del rack).	N/A	N/A
2.14	Para el cumplimiento de los ítems 1.5 al 2.30 el oferente deberá entregar documentación de fabricante de la marca que se ofrezca, donde se describan las características técnicas que satisfagan lo exigido; en el caso que algún fabricante maneje algunas funcionalidades diferentes pero que cumplan con lo solicitado, deberá demostrarlo con alguna documentación de fabricante.	N/A	N/A
2.15	CAPACIDAD OPERATIVA: El fin de garantizar la calidad de los elementos a adquirir y evitar incumplimientos en la ejecución del futuro contrato, se requiere que las firmas participantes en el proceso de selección cuenten con los mecanismos idóneos para el transporte, instalación y entrega inmediata de los elementos requeridos, una vez se efectúen los requerimientos por parte del supervisor del contrato, para lo cual deberá anexar en la oferta certificación de capacidad operativa expedida por el representante legal de la empresa.	N/A	N/A

2.16	TRANSFERENCIA DE CONOCIMIENTO: El proponente debe proveer capacitación certificada (curso de certificación de la plataforma de firewall ofertada), para cuatro (4) funcionarios de la entidad en centro de capacitación autorizado por el fabricante de los productos ofertados, con una intensidad de mínimo 35 horas, buscando la experticia en el manejo y funciones de administración en la herramienta. No se debe incluir los vouchers de certificación.	N/A	N/A
2.17	La trasferencia de conocimiento se debe brindar en las instalaciones que disponga el contratista, en acuerdo con el supervisor del contrato, en la ciudad de Bogotá de forma que se garantice la infraestructura adecuada.	N/A	N/A
2.18	EXPERIENCIA: Con el fin de garantizar el equipo adquirir y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente proceso, según el código de clasificación de los bienes, obras o servicios (UNSPSC) en la clasificación 43222500, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 621.98 S.M.M.L.V., de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).	N/A	N/A
2.19	EXPERIENCIA DEL PERSONAL: Se requiere que el personal profesional cuente con una experiencia en instalación, programación y configuración de la herramienta ofertada, para esto se debe anexar a la propuesta una (1) certificación por cada profesional, donde se evidencia su participación en proyectos similares al objeto del presente proceso durante los últimos tres (3) años (2020 y/o 2021 y/o 2022), estas certificaciones deberán ser expedidas por la empresa o entidad donde se desarrollaron los proyectos.	N/A	N/A
3	**CERTIFICACIÓN DEL FABRICANTE**		
3.1	El proponente deberá presentar una Certificación del fabricante donde conste que el proponente es un Canal Certificado, lo cual lo hace idóneo para diseñar, instalar y colocar en funcionamiento la solución presentada. El nivel mínimo deber ser su homologación de partner en nivel intermedio, lo que corresponde en las diferentes marcas, así: FORTINET - GOLD PARTNER o PALO ALTO –INNOVATOR o CISCO – PREMIER o CHECK POINT – TRES ESTRELLAS o su equivalente en las diferentes marcas.	N/A	N/A
3.2	El oferente debe anexar un documento expedido por el fabricante de los equipos ofrecidos, donde se especifique que los mismos son nuevos y tienen un ciclo de vida no inferior a cinco (5) años.	N/A	N/A
3.3	NIVEL ACADEMICO: El oferente deberá presentar en su oferta mínimo tres (3) profesionales en Ingeniería de Sistemas y/o Ingeniería en Telecomunicaciones y/o ingeniería Electrónica, por cada uno se deberá anexar fotocopia del diploma y/o acta de grado; de igual forma, se debe anexar al menos una (01) certificación en los niveles de experto, otorgados por fabricante de los equipos ofertados, dicha certificación se deberá adjuntar por cada uno de los profesionales (mínimo 03). NOTA: En caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia.	N/A	N/A
3.4	Servicios de Diseño e Implementación El proponente debe incluir en su propuesta servicios profesionales del fabricante para los temas de diseño e implementación el cual debe estar compuesto por al menos las siguientes actividades y entregables: Talleres de trabajo con el cliente: Recopilación de las necesidades del clientes y evaluación la red para determinar su capacidad para adoptar el sistema de control de acceso.	N/A	N/A
3.5	Diseño de alto nivel: Creación de un Diseño de Alto Nivel para la solución de control de acceso.	N/A	N/A
3.6	Diseño de Bajo nivel: Creación de un diseño de bajo nivel y con las recomendaciones de como el sistema de control de acceso debe ser implementado en cuanto a políticas y configuraciones mejorando las capacidades del sistema ofrecido.	N/A	N/A
3.7	Configuración basada en los requerimientos del cliente y el diseño elaborado por el fabricante.	N/A	N/A
3.8	Transferencia de información de la solución desplegada.	N/A	N/A
3.9	Todas las personas que hagan parte de las implementaciones por parte de la empresa a la que se le adjudique el contrato deben cumplir los protocolos de seguridad de la Seccional de Inteligencia Policial DICAR diligenciar el compromiso de reserva y estudios de seguridad, entre otros.	N/A	N/A
4	**ACUERDO DE CONFIDENCIALIDAD**		
4.1	El personal que realice la instalación y configuración de los equipos descritos en el presente proceso contractual, se someterá a un estudio de credibilidad y confiabilidad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato. En el evento de no cumplir o superar dicho estudio algunas de las personas vinculadas a este proyecto, el	N/A	N/A

	contratista realizará el cambio de estas personas por otras que también se someterán al estudio de credibilidad y confiabilidad requerida.		
4.2	Confidencialidad e integridad de la información institucional: dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista garantizará la preservación de la integridad y confidencialidad de la información institucional a la cual llegare a tener acceso directamente o por intermedio de terceros; en tal virtud, adoptará todas las medidas que sean necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida y suscribirá con la Entidad los formatos de confidencialidad o reserva a que haya lugar.	N/A	N/A
4.3	En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del futuro contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su labor. El contratista firmará un acuerdo de confidencialidad y no revelación de la información para lo cual diligenciará el formulario establecido por la entidad contratante	N/A	N/A
4.4	El manejo de toda la información de arquitectura de las herramientas se considera CONFIDENCIAL, de manera que los planos, diseño, manuales técnicos y cualquier otro tipo de información estarán limitados únicamente a la interventora o supervisión. El suministro de copias para otras personas o entidades será solicitado a la Seccional de Inteligencia Policial de la Policía Nacional.	N/A	N/A
4.5	El contratista y todo el personal que realice la instalación y configuración de los equipos, cumplirá los protocolos descritos en el Manual del Sistema de Gestión de Seguridad de la Información de la Policía Nacional y el instructivo vigente mediante el cual se establece el Protocolo de Seguridad de la Información para el Servicio de Inteligencia Policial, debiendo suscribir el compromiso de reserva y el de confidencialidad.	N/A	N/A
4.6	Durante el desarrollo de la instalación y configuración de los equipos, el contratista se compromete a no hacer uso indebido de las herramientas de software o hardware utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.	N/A	N/A
5	**ASPECTOS AMBIENTALES**		
5.1	El contratista deberá entregar los manuales de manera digital con el fin de aportar a la política cero papel establecida en directiva presidencial 04/2012.	N/A	N/A
5.2	El contratista deberá garantizar que los materiales de los empaques y/o embalajes estén constituidos con un porcentaje de material reciclable o provenir de una fuente sustentable no se permite el embalaje en componentes de ICOPOR.	N/A	N/A
5.3	Desarrollar y cumplir, durante la vigencia y ejecución del objeto del contrato, con las buenas prácticas ambientales con relación al ahorro y uso eficiente del agua y la energía, así como el manejo integral de residuos (no peligrosos y peligrosos), establecidas por la Dirección y el marco del mantenimiento del Sistema de Gestión Ambiental en las Instalaciones del Contratante; que contribuyan al cumplimiento de la política ambiental y objetivos ambientales institucionales.	N/A	N/A
6	**SEGURIDAD Y SALUD EN EL TRABAJO**		
6.1	• El contratista deberá entregar al supervisor del contrato el documento firmado por el representante legal el cual indique el número de trabajadores permanentes y el nivel de riesgo de su principal actividad económica, lo anterior como consideración a la Resolución 0312 del 13 de febrero del 2019 del Ministerio de Trabajo "Por la cual se definen los Estándares Mínimos del Sistema de Gestión de SST", en cumplimiento al art. 1 la presente Resolución tiene por objeto establecer los Estándares Mínimos del SG-SST para las personas naturales y jurídicas señaladas en el art. 2 aplica a los empleadores públicos y privados, a los contratantes del personal bajo modalidad de contrato civil, comercial o administrativo, a los trabajadores dependientes e independientes, a las organizaciones de economía solidaria y del sector cooperativo a las agremiaciones u asociaciones que afilian trabajadores independientes al sistema de seguridad social integral, a las empresas de servicios temporales, a los estudiantes afiliados al Sistema General de Riesgos Laborales y los trabajadores en misión; a las administradoras de riesgos laborales; a la Policía Nacional en lo que corresponde a su personal no uniformado y al personal civil de las Fuerzas Militares; quienes deben implementar los Estándares Mínimos del Sistema de Gestión de SST en el marco del Sistema de Garantía de Calidad del Sistema General de Riesgos Laborales. • El contratista deberá entregar al supervisor del contrato los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada. • El contratista deberá cumplir con los protocolos establecidos por el Ministerio de Salud y Protección Social en atención a la Resolución 1238 del 21/07/2022 "Por medio de la cual se	N/A	N/A

	dictan medidas para prevención, promoción y conservación de la salud con ocasión de infecciones respiratorias, incluidas las originadas por la COVID-19". • El contratista deberá garantizar que el personal que desarrolla las tareas durante la ejecución del cuente con los debidos Elementos de Protección Personal EPP, acorde a los peligros y riesgos relacionados la actividad contratada. • El contratista garantizará que el personal que desarrolle la tarea durante la ejecución del contrato, se encuentre con la debida identificación de la empresa. • En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al supervisor del contrato, con el fin de que este haga llegar la copia al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14/05/2007 del Ministerio de Trabajo y Protección Social "Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo" o cualquiera que la modifique, reemplace o sustituya. • El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato. • En caso de que se desarrolle en la Dirección de Inteligencia Policial una auditoría del SG-SST durante la ejecución del contrato, el contratista deberá suministrar al supervisor del contrato la documentación requerida del objeto contractual.		

2.1 NOVEDADES, SITUACIONES ANORMALES O DE RELEVANCIA

Mediante seguimiento al presente contrato de compraventa en el SECOP II, se evidenció que el señor Luis José Ignacio Quintero Cusguen representante legal de la empresa BOYAN S.A, solicita a la Dirección de Carabinero y Protección Ambiental prorroga de 30 días calendario al contrato 71-2-10038 cuyo objeto es "ADQUISICIÓN, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN DISPOSITIVO TIPO FIREWALL PARA LA SECCIONAL DE INTELIGENCIA POLICIAL DE LA DIRECCIÓN DE CARABINEROS Y PROTECCIÓN AMBIENTAL" por motivo de que la llegada de los equipos toma más tiempo del regularmente empleado por el fabricante.

3 AVANCE DE LA EJECUCIÓN DEL CONTRATO U ORDEN DE COMPRA:

A la fecha de corte 30 de noviembre de 2023, han transcurrido (37) días calendario desde que inicio el plazo de ejecución del contrato u orden de compra, restando (23) días calendario para que finalice el plazo de ejecución.

4 TRÁMITES Y VERIFICACIÓN DE PAGOS:

La Dirección de Carabineros y Protección Ambiental realizará el pago en moneda legal colombiana, de forma total, es decir, de acuerdo a la entrega del bien, una vez realizada la actividad, el contratista deberá entregar al supervisor del contrato, la factura y la certificación de aportes parafiscales conforme lo establece la Ley. Este, a su vez, expedirá el respectivo recibido a satisfacción y lo remitirá al Grupo Financiero de la Dirección de Carabineros y Protección Ambiental, junto con el informe de supervisión.

En todo caso el pago será realizado dentro de los sesenta (60) días siguientes a la radicación de los documentos relacionados con antelación, sujeto a la disponibilidad del Programa Anual de Caja (PAC). Aprobado por el Ministerio de Hacienda y Crédito Público y de acuerdo al derecho de turno contemplado en el Artículo 19 de la Ley 1150 de 2007, se aclara al oferente, que la administración verificará el estricto cumplimiento de los documentos que soporten el pago de los mismos, alejándose inclusive, del informe del supervisor para realizar el pago, si este tuviere inconsistencias dentro de los lineamientos establecidos para tal fin.

4.1. Ejecución Financiera y Pagos:

a. Balance general de pagos y entregas		
	Valor en pesos	**% del valor del contrato u orden de compra**
Valor total del contrato	$ 0	0%
Valor total de las entregas	$ 0	0%
Valor total facturado	$ 0	0%
Valor facturado pendiente de pago	$ 0	0%
Valor pagado	$ 0	0%
Valor pendiente de entrega	$ 0	0%

b. Detalle de las entregas, valores facturados y pagos efectuados en el periodo informado (la supervisión deberá relacionar de manera discriminada lo correspondiente a la ejecución del **únicamente del periodo que está informando**)

No. de acta o constancia de recibido	Valor recibido	Fecha de recibido	Valor facturado	No. factura	Valor pagado	Valor deducciones	No. orden de pago
Pendiente	Pendiente	Pendiente	Pendiente	Pendiente	Pendiente	Pendiente	Pendiente

4.2 Entrada de Bienes ***(verificar que los bienes hayan ingresado a los estados contables, si aplica)***

N/A

5 RECOMENDACIONES

N/A

El contratista cumplió con lo establecido en las cláusulas contractuales	**N/A**	Certifico con la firma del presente informe, que el contratista cumplió con las cláusulas y especificaciones técnicas del contrato, en la fecha o fechas establecidas, para lo cual relaciono y anexo los documentos soportes (técnicos obligatorios establecidos en las especificaciones técnicas, incluyendo las ambientales, de seguridad y salud en el trabajo y otros).
	N/A	En caso de incumplimiento parcial o total del contrato, se informó mediante comunicación oficial No. _____ Del _____, dirigida al ordenador del gasto, las obligaciones incumplidas.

6 CONCLUSIONES

El supervisor, deberá marcar con una (x) las casillas según corresponda al periodo entregado, con el fin de que la administración tenga claridad frente al cumplimiento o no del contratista. El no diligenciamiento será causal de la devolución del respectivo informe de supervisión.

Atentamente,

Firma_____

Capitán **FABIAN ESTEBAN MONTAÑA SARMIENTO**
Jefe de operaciones de la Seccional de Inteligencia Policial DICAR
Supervisor Contrato de compraventa 71-2-10038-23
Correo electrónico: fabian.montana1033@correo.policia.gov.co
Nro. Celular: 31674444604