



## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL DEL ECUADOR

### CONTRATO SCPN-AJ-026-2021

Comparecen a la celebración del presente contrato, por una parte el Servicio de Cesantía de la Policía Nacional del Ecuador, representado por el señor Coronel de Policía de E.M. Cristian Germán Barreiros Tumipamba, en calidad de Director Ejecutivo, a quien en adelante se le denominará CONTRATANTE o SCPN; y, por otra la empresa GREENDC S.A. con RUC 1792422426001, representada por su Gerente General señor Rubén Xavier Suquillo Armas, a quien en adelante se le denominará CONTRATISTA. Las partes se obligan en virtud del presente contrato, al tenor de las siguientes cláusulas:

#### **Cláusula Primera.- ANTECEDENTES.**

**1.1** De conformidad con los artículos 22 de la Ley Orgánica del Sistema Nacional de Contratación Pública -LOSNC-P-, y 25 y 26 de su Reglamento General -RGLOSNC-P-, el Plan Anual de Contrataciones de la CONTRATANTE, contempla la "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN".

**1.2.** Previo los informes y los estudios respectivos, la máxima autoridad de la CONTRATANTE resolvió aprobar el pliego de SUBASTA INVERSA ELECTRÓNICA SIE-SCPN-2021-003 para la "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN".

**1.3** Se cuenta con la existencia y suficiente disponibilidad de fondos en la partida presupuestaria en los siguientes rubros: código 840107, Equipos, Sistemas y Paquetes Informáticos, para el proceso de "Adquisición de equipos de seguridad informática para el SCPN", conforme consta en la certificación conferida por el Departamento Financiero del Servicio de Cesantía de la Policía Nacional mediante Oficio No. SCPN-EF-PRES/CERT-047-2021, de fecha 05 de mayo de 2021.

**1.4** Se realizó la respectiva convocatoria el 2021-06-07, a través del Portal Institucional.

**1.5** Luego del proceso correspondiente, el señor Coronel de Policía de E.M. Cristian Germán Barreiros Tumipamba, en su calidad de máxima autoridad de la CONTRATANTE, mediante resolución No. SCPN-DE-AJ-007-2021 de 30 de junio de 2021, adjudicó la "ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN".

#### **Cláusula Segunda.- DOCUMENTOS DEL CONTRATO.**

**2.1** Forman parte integrante del contrato los siguientes documentos:

- a) El pliego (Condiciones Particulares del Pliego CPP y Condiciones Generales del Pliego CGP) incluyendo las especificaciones técnicas, o términos de referencia del objeto de la contratación.
- b) Las Condiciones Generales de los Contratos de adquisición de bienes o prestación de servicios (CGC) publicados y vigentes a la fecha de la convocatoria en la página institucional del SERCOP.
- c) La oferta presentada por el CONTRATISTA, con todos sus documentos que la

[www.cesantiapn.com.ec](http://www.cesantiapn.com.ec)

Quito: Av. 9 de Octubre N29-24 y Eloy Alfaro

02 3 950 900

Guayaquil: Pedro Moncayo 1002 y José Vélaz

04 2 329 288 / 04 2 329 363





conforman.

- d) Las garantías presentadas por el CONTRATISTA.
- e) La resolución de adjudicación.
- f) Las certificaciones de la señora Jefa del Departamento Financiero del Servicio de Cesantía de la Policía Nacional, que acrediten la existencia de la partida presupuestaria y disponibilidad de recursos, para el cumplimiento de las obligaciones derivadas del contrato.
- g) Los documentos que acreditan la calidad de los comparecientes y su capacidad para celebrar el contrato.

### **Cláusula Tercera.- OBJETO DEL CONTRATO.**

**3.01** El Contratista se obliga con el contratante a proveer de equipos de seguridad informática para el SCPN y ejecutar el contrato a entera satisfacción de la contratante, en el lugar que le sea indicado, según las características y especificaciones técnicas constantes en la oferta, pliegos y términos de referencia que se agrega y forma parte integrante de este contrato.

### **Cláusula Cuarta.- PRECIO DEL CONTRATO.**

**4.1** El valor del presente contrato, que la CONTRATANTE pagará al CONTRATISTA, es el de USD 17.500,00 (diecisiete mil quinientos con 00/100) dólares de los Estados Unidos de América más IVA, con un plazo de ejecución de 45 días calendario contados a partir de la suscripción del contrato, de conformidad con la oferta presentada por el CONTRATISTA.

PRODUCTOS Y SERVICIOS ESPERADOS			
Detalle de los bienes esperados			
Cantidad	Descripción	Especificaciones técnicas requeridas	
		Equipo	Precio Unitario más IVA
		Firewall Fortinet 200F	





1  <b>FIREWALL NGFW FORTINET 200F</b>	Modelo	<p>El modelo de Firewall ofertado debe ser nuevo de fábrica, no remanufacturado, de las últimas familias de hardware lanzadas al mercado por el fabricante, por lo que no debe tener “End of Sale” (Fin de venta) ni “End of Support” (Fin de soporte) anunciado por el fabricante, o por discontinuarse en los próximos 12 meses. Así como también deberá garantizar la disponibilidad de partes y piezas, acceso a actualizaciones de firmware y versiones, parches para el tiempo de duración del contrato. Así como también debe estar catalogado como UTM.</p> <p>El fabricante de la solución ofertada deberá estar calificado como líder en el cuadrante mágico de Gartner más reciente (2020) para Enterprise Network Firewalls e Infraestructura WAN Edge, garantizando así que el equipo ofertado sea líder en la industria de seguridad.</p>	15.759,00
	Arquitectura	<p>Deberán contar con procesadores SPU que garanticen el poder detectar contenidos maliciosos a velocidades multi-Gigabit. Se requiere de estos procesadores SPU, pues proporcionan el rendimiento necesario para bloquear amenazas emergentes, y aseguran que la solución de seguridad de la red no se convierta en un cuello de botella.</p> <p>La solución ofertada debe contar con todo el hardware, software y licenciamiento necesario por 3 años para brindar las siguientes funcionalidades:</p> <ul style="list-style-type: none"><li>- IPS.</li><li>- Control de aplicaciones</li><li>- Filtrado Web.</li><li>- Antispam.</li><li>- Protección de amenazas avanzadas de malware.</li><li>- Protección en la nube de seguridad Sandboxing contra amenazas de día cero.</li><li>- Inspección SSL.</li></ul> <p>Los dispositivos no deben ser licenciado para funcionalidades de Routing como enrutamiento estático o VPN IPsec.</p>	





	Tipo	<p>El hardware de la plataforma de seguridad debe ser de tipo Appliance (hardware y software integrados del mismo fabricante). (No se aceptan soluciones virtualizadas).</p> <p>La solución que compone la plataforma de seguridad, se debe entender como el hardware y licenciamiento de software necesarios para su funcionamiento.</p> <p>El equipo debe ser de tipo rackeable en un rack de 19 pulgadas. Se debe incluir todos los accesorios para el montaje en el rack.</p>
	Administración	<p>La solución de Firewall debe ser accesible a través de SSH y de interfaz Web usando SSL.</p>
	Características de Red	<p>El appliance ofertado debe contar con las siguientes características de red:</p> <ul style="list-style-type: none"><li>• Debe incluir como mínimo:<ul style="list-style-type: none"><li>- 16 interfaces GE RJ45</li><li>- 1 interfaz GE RJ45 MGMT, 1</li><li>- 1 puerto USB.</li><li>- 1 puerto de consola.</li><li>- 2 slots 10 GE SFP+.</li><li>- 8 slots GE SFP</li></ul></li></ul>
	Características de Despliegue	<p>La solución ofertada debe permitir el despliegue a través de dos posibles configuraciones:</p> <ul style="list-style-type: none"><li>- Next Generation Firewall (NGFW).</li><li>- Secure SD-WAN</li><li>- Secure Web Gateway</li></ul>





		<p>El Next Generation Firewall (NGFW) debe permitir realizar lo siguiente:</p> <ul style="list-style-type: none"><li>- Bloquear automáticamente amenazas de tráfico descifrado utilizando inspección SSL, que incluya el estándar TLS 1.3 con cifrado obligatorio.</li><li>- Identificar y detener amenazas con una poderosa prevención de intrusos más allá de puerto y protocolo que examina el contenido real de su tráfico de red.</li><li>- Bloquear proactivamente los ataques sofisticados recientemente descubiertos en tiempo real con tecnologías de inteligencia artificial y servicios de amenazas avanzadas.</li></ul>	
		<p>El Secure SD-WAN debe permitir realizar lo siguiente:</p> <ul style="list-style-type: none"><li>- Acceso a múltiples nubes para una rápida adopción de servicios SaaS.</li><li>- Redes autoreparables con alta disponibilidad de enlaces WAN.</li><li>- Rendimiento constante de las aplicaciones empresariales mediante el direccionamiento dinámico de la mejor ruta WAN.</li></ul>	
		<p>El Secure Web Gateway debe permitir realizar:</p> <ul style="list-style-type: none"><li>- Asegurar el acceso a Webs para tráfico cifrado de alto rendimiento.</li><li>- Experiencia de usuario con almacenamiento de cache web.</li><li>- Bloquear y controlar el acceso a la web en función de usuarios o grupo de usuarios.</li><li>- Evitar la pérdida de datos y descubrir la actividad del usuario de forma conocida y aplicaciones en la nube desconocidas.</li></ul>	





	Características eléctricas	Por lo menos que soporte fuente de poder redundante.
	Dashboard	Monitorear recurso, RAM, almacenamiento, procesamiento, conexiones de red por interfaces. Perfiles asignados Aplicaciones más utilizadas Consumo de ancho de banda Sesiones concurrentes Alertas de eventos Notificaciones
	Procesador de Red	Debe contar con un nuevo y revolucionario procesador de red SPU NP, el cual debe funcionar en línea con la entrega de ciertas funciones del Sistema operativo. - SPU: NP6X Lite o superior
		Deben entregar un funcionamiento superior de firewall para todo tipo de cargas IP y tramas de Ethernet.
		Deben soportar cifrado VPN y aceleración del túnel IP. Deben entregar un funcionamiento superior con prevención de intrusiones basadas en anomalías, descarga de suma de comprobación y desfragmentación de paquetes.
	Procesador de contenido	El procesador de contenido debe ser SPU CP debido a que funciona afuera del flujo directo de tráfico. <ul style="list-style-type: none"><li>• El procesador de contenido debe proporcionar criptografía de alta velocidad e inspección de contenido, con un servicio que incluya:<ul style="list-style-type: none"><li>- Rendimiento IPS mejorado con capacidad única de completa coincidencia de firmas ASIC.</li><li>- Descarga de cifrado y descifrado.</li><li>- Capacidad de Inspección SSL.</li></ul></li></ul>





	Networking	<p>La solución ofertada debe garantizar y soportar las siguientes especificaciones:</p> <ul style="list-style-type: none"><li>• Latencia de Firewall: 4.78 us</li><li>• Nuevas sesiones por segundo (TCP): 280.000</li><li>• Seguridad: protección avanzada contra malware</li><li>• Rendimiento para IPv4/IPv6, Vlan</li><li>• DHCP Cliente y Servidor DHCP</li><li>• Políticas de enrutamiento</li><li>• NAT</li><li>• Enrutamiento dinámico</li><li>• Soporte: 500 Túneles VPN SSL</li><li>• La solución de Firewall ofertada debe ser capaz de realizar Backup/Restore de la configuración</li><li>• La solución ofertada deberá tener un módulo dedicado para almacenar y autenticar claves criptográficas para protección de ataques maliciosos y ataques de phishing.</li></ul>
	Desempeño por Gateway	Debe tener IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) mínima de 27 / 27 / 11 Gbps
		Debe soportar al menos 3 Millones de Sesiones Concurrente (TCP).
		Debe soportar al menos 13 Gbps de Throughput de VPN IPSec.
		Debe soportar al menos un Performance de: - IPS Throughput:5 Gbps - NGFW Throughput:3,5 Gbps - Rendimiento de Protección contra amenazas: 3 Gbps
		Debe soportar al menos 10.000 de Políticas de Firewall.
	Informes	Debe soportar al menos 4 Gbps de SSL Inspection Throughput (IPS, HTTPS).
	Servicios de seguridad	Crear reportes que puedan ser programados para ser enviados por correo electrónico de manera automática.
		El fabricante debe ofrecer a través de Laboratorios distribuidos por todo el mundo, una inteligencia en tiempo real sobre las amenazas, ofreciendo actualizaciones de seguridad completas.





	Soporte	<p>La solución ofertada incluye:</p> <p>Soporte, garantía y licenciamiento de fábrica por 3 años a nivel hardware y software en modalidad 24x7.</p> <ul style="list-style-type: none"><li>• Métodos de respuesta: Teléfono/correo electrónico, soporte remoto.</li><li>• Debe contar con un sistema de soporte online provisto por el fabricante.</li><li>• Contar con un sistema de soporte online provisto por el oferente local.</li><li>• Instalación y configuración con las políticas de seguridad que se le entregarán a la empresa adjudicada para la puesta en marcha del equipo.</li><li>• A partir de la recepción, el proveedor adjudicado se compromete a realizar la transferencia de conocimientos a dos funcionarios del Departamento de TIC's, con objeto de conseguir la información completa de la instalación, administración, configuración, operatividad y manejo de la solución Firewall ofertada, por el tiempo de al menos 8 horas y entregará un certificado de capacitación abalado por el profesional especialista en seguridad informática experimentado en la administración del equipo ofertado. (La capacitación será en las instalaciones del SCPN).</li></ul>							
	Modelo	<table><tr><th>Equipo</th><th>Precio Unitario más IVA</th></tr><tr><td><b>Especificar: Switch Cisco SG220-50P 50-Port Gigabit POE incluye 2 transceiver Gigabit Ethernet MGBSX1.</b></td><td></td></tr><tr><td colspan="2">El modelo de switch ofertado debe ser nuevo de fábrica, no remanufacturado, no debe tener “End of Sale” (Fin de venta) ni “End of Support” (Fin de soporte) anunciado por el fabricante, o por discontinuarse en los próximos 12 meses. Así como también deberá garantizar la disponibilidad de partes y piezas, acceso a actualizaciones de firmware y versiones, parches para el tiempo de duración del contrato.</td></tr></table>	Equipo	Precio Unitario más IVA	<b>Especificar: Switch Cisco SG220-50P 50-Port Gigabit POE incluye 2 transceiver Gigabit Ethernet MGBSX1.</b>		El modelo de switch ofertado debe ser nuevo de fábrica, no remanufacturado, no debe tener “End of Sale” (Fin de venta) ni “End of Support” (Fin de soporte) anunciado por el fabricante, o por discontinuarse en los próximos 12 meses. Así como también deberá garantizar la disponibilidad de partes y piezas, acceso a actualizaciones de firmware y versiones, parches para el tiempo de duración del contrato.		
Equipo	Precio Unitario más IVA								
<b>Especificar: Switch Cisco SG220-50P 50-Port Gigabit POE incluye 2 transceiver Gigabit Ethernet MGBSX1.</b>									
El modelo de switch ofertado debe ser nuevo de fábrica, no remanufacturado, no debe tener “End of Sale” (Fin de venta) ni “End of Support” (Fin de soporte) anunciado por el fabricante, o por discontinuarse en los próximos 12 meses. Así como también deberá garantizar la disponibilidad de partes y piezas, acceso a actualizaciones de firmware y versiones, parches para el tiempo de duración del contrato.									







1  SWITCH CISCO SG220-50P 50- PORT GIGABIT POE, INCLUYE 2 TRANSCEIVER GIGABIT ETHERNET MGBSX1	Rendimiento	<ul style="list-style-type: none"><li>- Debe contar con memoria de CPU de 128 MB o superior.</li><li>- Debe soportar una memoria flash de 32 MB o superior.</li><li>- Debe soportar al menos una tasa de retransmisión expresada en millones de paquetes por segundo (mpps; basada en paquetes de 64 bytes): 74,40</li></ul>	1.741,00
	Switching de capa 2	<ul style="list-style-type: none"><li>- Debe soportar un máximo de 256 VLAN activas simultáneas.</li><li>- VLAN basadas en puertos y en etiquetas 802.1Q</li><li>- Gestión de VLAN</li></ul>	
		<ul style="list-style-type: none"><li>- Debe tener compatibilidad con el protocolo de árbol de extensión 802.1d estándar.</li></ul>	
	Seguridad	Debe soportar Listas de control de acceso (ACL) de hasta 512 reglas.	
		Debe tener capacidad de bloquear direcciones MAC de origen a los puertos y limitar el número de direcciones MAC detectadas.	
		Debe contar con la funcionalidad de prevención de ataques de denegación de servicio DoS.	
		Debe ser compatible con filtrado de dirección MAC.	
		Debe contar con protección de sesiones de administración mediante RADIUS y TACACS+, y compatibilidad con autenticación local de bases de datos, así como con sesiones de administración segura a través de SSL, SSH y SNMP v3.	





Características de Red	<p>El equipo ofertado debe contar con las siguientes características de red mínimas:</p> <ul style="list-style-type: none"><li>- 48 puertos 10/100/1000 PoE con 375 W de presupuesto energético.</li><li>- 2 puertos combinados Gigabit RJ45/SFP Compatibilidad con Power over Ethernet 802.3 af, 802.3 at.</li><li>- INCLUYE 2 TRANSCEIVER GIGABIT ETHERNET para Fibra Multimodo de distancia máxima 550 m (MGBSX1) (Los módulos deben ser de última generación, nuevos de fábrica, no remanufacturados (no refurbished), ni reparados, ni reacondicionados en ninguna de sus partes o componentes.), compatible con el Switch ofertado.</li></ul>	
Administración	<p>El equipo ofertado debe contar mínimo con:</p> <ul style="list-style-type: none"><li>- Administración remota</li><li>- Interfaz de línea de comandos (CLI).</li><li>- Interfaz de usuario web.</li><li>- Soportar SNMP versiones 1.2c y 3.</li><li>- Coexistencia de ambas pilas de protocolos para facilitar la migración de IPv4/IPv6.</li><li>- Soportar QoS.</li><li>- Compatibilidad con telefonía IP.</li></ul>	
Soporte	<p>La solución ofertada incluye: Soporte y garantía por 3 años. El equipo debe contar con soporte del fabricante para actualizaciones de seguridad todo el tiempo de duración de la garantía del equipo.</p>	
Subtotal		17.500,00
IVA		2.100.00
VALOR TOTAL		19.600,00

**4.2** Los precios acordados en el contrato, constituirán la única compensación al CONTRATISTA por todos sus costos, inclusive cualquier impuesto, derecho o tasa que tuviese que pagar, excepto el Impuesto al Valor Agregado que será añadido al precio del contrato conforme se menciona en el numeral 4.1.

#### **Cláusula Quinta.- FORMA DE PAGO.**

Se pagará al oferente el 100% contra entrega de los productos, previa firma del acta de entrega recepción definitiva de los equipos, entrega de garantías correspondientes, presentación de la factura e informe de satisfacción del administrador del contrato.

[www.cesantiapn.com.ec](http://www.cesantiapn.com.ec)

Quito: Av. 9 de Octubre N29-24 y Eloy Alfaro

02 3 950 900

Guayaquil: Pedro Moncayo 1002 y José Vélez

04 2 329 288 / 04 2 329 363





### **Cláusula Sexta.- GARANTÍAS.**

**6.1** En este contrato se rendirán la garantía técnica de todos los bienes por el plazo de 3 años, misma que entrara en vigencia a partir de la entrega recepción de los bienes, conforme el artículo 76 de la LOSNCP, además en sujeción a los artículos desde 114 hasta el artículo 125 de la Resolución Nro. RE-SERCOP-2016-0000072, términos de referencia de los pliegos, y, la oferta del contratista, en el ítem Garantía Técnica, soporte y mantenimientos.

**6.2** Las garantías entregadas se devolverán de acuerdo a lo establecido en el artículo 118 del RGLOSNCP. Entre tanto, deberán mantenerse vigentes, lo que será vigilado y exigido por la CONTRATANTE.

### **Cláusula Séptima.- PLAZO.**

El plazo para la prestación de los servicios contratados a entera satisfacción de la CONTRATANTE es de 45 días calendario contados a partir de la suscripción del contrato.

### **Cláusula Octava.- MULTAS.**

Por cada día de retardo en la ejecución de las obligaciones contractuales por parte del Contratista, se aplicará la multa del 1 por 1.000 del valor del contrato de conformidad al artículo 71 de la LOSNCP y artículo 116 del RGLOSNCP.

### **Cláusula Novena.- DEL REAJUSTE DE PRECIOS.**

El presente contrato no contempla reajuste de precios, por lo tanto, conforme a lo estipulado en el artículo 131, segundo inciso del Reglamento a la LOSNCP, el CONTRATISTA, renuncia expresamente a cualquier reclamo por dicho concepto en el presente instrumento.

### **Cláusula Décima.- DE LA ADMINISTRACIÓN DEL CONTRATO.**

**10.1** La CONTRATANTE designa a la Ing. Viviana Elizabeth Ayala Yandún, Analista de Infraestructura y Redes, en calidad de administradora del contrato, quien deberá atenerse a las condiciones generales y particulares de los pliegos que forman parte del presente contrato.

**10.2** LA CONTRATANTE podrá cambiar de administrador del contrato, para lo cual bastará cursar al CONTRATISTA la respectiva comunicación; sin que sea necesario la modificación del texto contractual.

### **Cláusula Undécima.- TERMINACIÓN DEL CONTRATO**

**11.1 Terminación del contrato.-** El contrato termina conforme lo previsto en el artículo 92 de la Ley Orgánica del Sistema Nacional de Contratación Pública y las Condiciones Particulares y Generales del Contrato.

**11.2 Causales de Terminación unilateral del contrato.-** Tratándose de incumplimiento del CONTRATISTA, procederá la declaración anticipada y unilateral de la CONTRATANTE, en los casos establecidos en el artículo 94 de la LOSNCP. Además, se considerarán las





siguientes causales:

- a) Si el CONTRATISTA no notificare a la CONTRATANTE acerca de la transferencia, cesión, enajenación de sus acciones, participaciones, o en general de cualquier cambio en su estructura de propiedad, dentro de los cinco días hábiles siguientes a la fecha en que se produjo tal modificación;
- b) Si la CONTRATANTE, en función de aplicar lo establecido en el artículo 78 de la LOSNCP, no autoriza la transferencia, cesión, capitalización, fusión, absorción, transformación o cualquier forma de tradición de las acciones, participaciones o cualquier otra forma de expresión de la asociación, que represente el veinticinco por ciento (25%) o más del capital social del CONTRATISTA;
- c) Si se verifica, por cualquier modo, que la participación ecuatoriana real en la provisión de bienes o prestación de servicios objeto del contrato es inferior a la declarada.
- d) Si el CONTRATISTA incumple con las declaraciones que ha realizado en el numeral 3.5 del formulario de la oferta - Presentación y compromiso;
- e) El caso de que la entidad contratante encuentre que existe inconsistencia, simulación y/o inexactitud en la información presentada por contratista, en el procedimiento precontractual o en la ejecución del presente contrato, dicha inconsistencia, simulación y/o inexactitud serán causales de terminación unilateral del contrato por lo que, la máxima autoridad de la entidad contratante o su delegado, lo declarará contratista incumplido, sin perjuicio además, de las acciones judiciales a que hubiera lugar.

**11.3 Procedimiento de terminación unilateral.-** El procedimiento a seguirse para la terminación unilateral del contrato será el previsto en el artículo 95 de la LOSNCP.

#### **Cláusula Duodécima.- SOLUCIÓN DE CONTROVERSIAS.**

**12.1** Si respecto de la divergencia o controversia existentes no se lograre un acuerdo directo entre las partes, éstas se someterán al procedimiento establecido en el COGEP; siendo competente para conocer la controversia el Tribunal Distrital de lo Contencioso Administrativo que ejerce jurisdicción en el domicilio de la Entidad Contratante.

**12.2** La legislación aplicable a este contrato es la ecuatoriana. En consecuencia, el contratista declara conocer el ordenamiento jurídico ecuatoriano y por lo tanto, se entiende incorporado el mismo en todo lo que sea aplicable al presente contrato.

#### **Cláusula Décima Tercera: COMUNICACIONES ENTRE LAS PARTES.**

**13.1** Todas las comunicaciones, sin excepción, entre las partes, relativas a los trabajos, serán formuladas por escrito y en idioma castellano. Las comunicaciones entre la administración y el CONTRATISTA se harán a través de documentos escritos.

#### **Cláusula Décima Cuarta.- DOMICILIO.**

**14.1.** Para todos los efectos de este contrato, las partes convienen en señalar su domicilio en la ciudad de Quito.

[www.cesantiapn.com.ec](http://www.cesantiapn.com.ec)

Quito: Av. 9 de Octubre N29-24 y Eloy Alfaro

02 3 950 900

Guayaquil: Pedro Moncayo 1002 y José Vélaz

04 2 329 288 / 04 2 329 363





Servicio de Cesantía  
de la Policía Nacional

**14.2.** Para efectos de comunicación o notificaciones, las partes señalan como su dirección, las siguientes:

La CONTRATANTE: Quito. Avenida 9 de octubre N29-24 y Eloy Alfaro. Teléfono 023950900, Email: sistemas@cesantiapn.com.ec

El CONTRATISTA: Quito, Av. Mariscal Sucre N71-282 y José Miguel Carrión; Email: xavier.suquillo@greendc.com.ec; Teléfono: 0996481752.

Las comunicaciones también podrán efectuarse a través de medios electrónicos.

#### **Cláusula Décima Quinta.- ACEPTACIÓN DE LAS PARTES.**

**15.1 Declaración.-** Las partes libre, voluntaria y expresamente declaran que conocen y aceptan el texto íntegro de las Condiciones Generales de los Contratos de provisión de bienes y prestación de servicios, publicado en la página institucional del Servicio Nacional de Contratación Pública SERCOP, vigente a la fecha de la Convocatoria del procedimiento de contratación, y que forma parte integrante de las Condiciones Particulares del Contrato que lo están suscribiendo.

**15.2.** Libre y voluntariamente, las partes expresamente declaran su aceptación a todo lo convenido en el presente contrato y se someten a sus estipulaciones.

Dado, en la ciudad de Quito, a los nueve días del mes de julio de 2021.



Firmado electrónicamente por:  
**CRISTIAN GERMAN  
BARREIROS  
TUMIPAMBA**

Cristian Germán Barreiros Tumipamba  
Coronel de Policía de E.M  
**DIRECTOR EJECUTIVO DEL SERVICIO  
DE CESANTÍA DE LA POLICÍA  
NACIONAL  
CONTRATANTE**



Firmado electrónicamente por:  
**RUBEN XAVIER  
SUQUILLO  
ARMAS**

Rubén Xavier Suquillo Armas  
**Gerente General  
GREENDC S.A.  
RUC 1792422426001  
CONTRATISTA**

[www.cesantiapn.com.ec](http://www.cesantiapn.com.ec)

Quito: Av. 9 de Octubre N29-24 y Eloy Alfaro  
02 3 950 900

Guayaquil: Pedro Moncayo 1002 y José Vélaz  
04 2 329 288 / 04 2 329 363



## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL DEPARTAMENTO DE TECNOLOGÍA

### ACTA DE ENTREGA RECEPCIÓN DEFINITIVA

**CONTRATO:** SCPN-AJ-026-2021

**FECHA DE ADJUDICACIÓN:** 09-07-2021

**FECHA DE INICIO:** 09-07-2021

**FECHA MÁXIMA DE ENTREGA DE EQUIPOS:** 23-08-2021

**OBJETO DE LA CONTRATACIÓN:** El contratista se obliga con el Servicio de Cesantía de la Policía Nacional a proveer la “**ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN**”, y a ejecutar el contrato a entera satisfacción de la contratante, según los términos de referencia constantes en la oferta, que se agrega y forma parte integrante de esta contratación.

**VALOR DE LA CONTRATACIÓN:** \$17.500,00 (Diecisiete mil quinientos con 00/100) más IVA.

**NOMBRE DEL REPRESENTANTE LEGAL DEL PROVEEDOR ADJUDICADO:** Ing. Ruben Xavier Suquillo Armas.

**TIPO DE PROCESO DE CONTRATACIÓN:** Subasta Inversa Electrónica.

#### 1. ANTECEDENTES

- Existe Resolución de Adjudicación Nro. SCPN-DE-AJ-007-2021 para la “**ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN**”, de fecha 29 de junio de 2021 suscrita por el señor Coronel de Policía de E.M. Cristian Germán Barreiros Tumipamba, Director Ejecutivo del SCPN.
- Existe Contrato Nro. SCPN-AJ-026-2021 para la “**ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN**”, de fecha 09 de julio de 2021 suscrito por el señor Coronel de Policía de E.M. Cristian Germán Barreiros Tumipamba, Director Ejecutivo del SCPN y el señor Ing. Ruben Xavier Suquillo Armas, Representante Legal de la empresa GREENDC S.A.
- Existe oficio Nro. SCPN-CP-113-2021 de fecha 09 de julio de 2021, suscrita por el señor señor Mayor de Policía Héctor Mauricio Cedeño Arévalo, Jefe de Compras Públicas del SCPN encargado, mediante el cual se notifica como Administradora del Contrato Nro. SCPN-AJ-026-2021, a la Ing. Viviana Ayala Yandún y al señor Ing. Raul Alejandro Rodriguez Parra como Técnico miembro de la comisión de recepción.
- Existe un oficio Nro. SCPN-TIC-AR-039-2021 de fecha 11 de agosto de 2021, suscrito por la Ing. Viviana Ayala Yandún, Administradora del Contrato Nro. SCPN-AJ-026-2021, mediante el cual se solicita el ingreso provisional a Bodega.
- Existe memorando Nro. SCPN-DA-281-2021 de fecha 13 de agosto de 2021, suscrito por la señorita Subteniente de Policía Lezlie Romero Anchatipán, Jefe Administrativo Subrogante, en el cual remite el ingreso provisional a bodega Nro. 2021-13.

#### 2. CONDICIONES GENERALES DE EJECUCIÓN

Dando cumplimiento al detalle del Contrato N° SCPN-AJ-026-2021 del proceso “**ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN**”, se pone en conocimiento que se ha recibido lo detallado en la siguiente tabla, conjuntamente la Administradora del Contrato y el Técnico



## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

miembro de la comisión de recepción designados mediante oficio Nro. SCPN-CP-113-2021 de fecha 09 de julio de 2021:

DETALLE DE LOS BIENES ESPERADOS		
Detalle	Descripción	Especificaciones técnicas requeridas
<b>1 FIREWALL NGFW FORTINET 200F</b>	Modelo	<p>Equipo: Firewall Fortinet 200F</p> <p>El modelo de Firewall recibido es nuevo de fábrica, no remanufacturado, de las últimas familias de hardware lanzadas al mercado por el fabricante, por lo que no debe tener "End of Sale" (Fin de venta) ni "End of Support" (Fin de soporte) anunciado por el fabricante, o por discontinuarse en los próximos 12 meses. Así como también deberá garantizar la disponibilidad de partes y piezas, acceso a actualizaciones de firmware y versiones, parches para el tiempo de duración del contrato. Así como también debe estar catalogado como UTM.</p> <p>El fabricante de la solución ofertada deberá estar calificado como líder en el cuadrante mágico de Gartner más reciente (2020) para Enterprise Network Firewalls e Infraestructura WAN Edge, garantizando así que el equipo ofertado sea líder en la industria de seguridad.</p>
	Arquitectura	<p>Deberán contar con procesadores SPU que garanticen el poder detectar contenidos maliciosos a velocidades multi-Gigabit. Se requiere de estos procesadores SPU, pues proporcionan el rendimiento necesario para bloquear amenazas emergentes, y aseguran que la solución de seguridad de la red no se convierta en un cuello de botella.</p> <p>La solución cuenta con todo el hardware, software y licenciamiento necesario por 3 años para brindar las siguientes funcionalidades:</p> <ul style="list-style-type: none"> <li>- IPS.</li> <li>- Control de aplicaciones</li> <li>- Filtrado Web.</li> <li>- Antispam.</li> <li>- Protección de amenazas avanzadas de malware.</li> <li>- Protección en la nube de seguridad Sandboxing contra amenazas de día cero.</li> <li>- Inspección SSL.</li> </ul> <p>Los dispositivos no deben ser licenciado para funcionalidades de Routing como enrutamiento estático o VPN IPsec.</p>
	Tipo	<p>El hardware de la plataforma de seguridad es de tipo Appliance (hardware y software integrados del mismo fabricante). (No se aceptan soluciones virtualizadas).</p> <p>La solución que compone la plataforma de seguridad, se debe entender como el hardware y licenciamiento de software necesarios para su funcionamiento.</p> <p>El equipo es de tipo rackeable en un rack de 19 pulgadas. Se debe incluir todos los accesorios para el montaje en el rack.</p>
	Administración	La solución de Firewall es accesible a través de SSH y de interfaz Web usando SSL.
	Características de Red	<p>El appliance cuenta con las siguientes características de red:</p> <ul style="list-style-type: none"> <li>• Incluye como mínimo: <ul style="list-style-type: none"> <li>- 16 interfaces GE RJ45</li> <li>- 1 interfaz GE RJ45 MGMT, 1</li> <li>- 1 puerto USB.</li> <li>- 1 puerto de consola.</li> <li>- 2 slots 10 GE SFP+.</li> <li>- 8 slots GE SFP</li> </ul> </li> </ul>
	Características de Despliegue	<p>La solución permite el despliegue a través de dos posibles configuraciones:</p> <ul style="list-style-type: none"> <li>- Next Generation Firewall (NGFW).</li> <li>- Secure SD-WAN</li> <li>- Secure Web Gateway</li> </ul> <p>El Next Generation Firewall (NGFW) permite realizar lo siguiente:</p> <ul style="list-style-type: none"> <li>- Bloquear automáticamente amenazas de tráfico descifrado utilizando inspección SSL, que incluya el estándar TLS 1.3 con cifrado obligatorio.</li> <li>- Identificar y detener amenazas con una poderosa prevención de intrusos más allá de puerto y protocolo que examina el contenido real de su tráfico de red.</li> <li>- Bloquear proactivamente los ataques sofisticados recientemente descubiertos en tiempo real con tecnologías de inteligencia artificial y servicios de amenazas avanzadas.</li> </ul>



## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

	<p>El Secure SD-WAN debe permitir realizar lo siguiente:</p> <ul style="list-style-type: none"><li>- Acceso a múltiples nubes para una rápida adopción de servicios SaaS.</li><li>- Redes autoreparables con alta disponibilidad de enlaces WAN.</li><li>- Rendimiento constante de las aplicaciones empresariales mediante el direccionamiento dinámico de la mejor ruta WAN.</li></ul>
	<p>El Secure Web Gateway permite realizar:</p> <ul style="list-style-type: none"><li>- Asegurar el acceso a Webs para tráfico cifrado de alto rendimiento.</li><li>- Experiencia de usuario con almacenamiento de cache web.</li><li>- Bloquear y controlar el acceso a la web en función de usuarios o grupo de usuarios.</li><li>- Evitar la pérdida de datos y descubrir la actividad del usuario de forma conocida y aplicaciones en la nube desconocidas.</li></ul>
Características eléctricas	Soporta fuente de poder redundante.
Dashboard	Monitorear recurso, RAM, almacenamiento, procesamiento, conexiones de red por interfaces. Perfiles asignados Aplicaciones más utilizadas Consumo de ancho de banda Sesiones concurrentes Alertas de eventos Notificaciones
Procesador de Red	<p>Debe contar con un nuevo y revolucionario procesador de red SPU NP, el cual debe funcionar en línea con la entrega de ciertas funciones del Sistema operativo.</p> <ul style="list-style-type: none"><li>- SPU: NP6X Lite o superior</li></ul> <p>Deben entregar un funcionamiento superior de firewall para todo tipo de cargas IP y tramas de Ethernet.</p> <p>Deben soportar cifrado VPN y aceleración del túnel IP.</p> <p>Deben entregar un funcionamiento superior con prevención de intrusiones basadas en anomalías, descarga de suma de comprobación y desfragmentación de paquetes.</p>
Procesador de contenido	<p>El procesador de contenido debe ser SPU CP debido a que funciona afuera del flujo directo de tráfico.</p> <ul style="list-style-type: none"><li>• El procesador de contenido debe proporcionar criptografía de alta velocidad e inspección de contenido, con un servicio que incluya:<ul style="list-style-type: none"><li>- Rendimiento IPS mejorado con capacidad única de completa coincidencia de firmas ASIC.</li><li>- Descarga de cifrado y descifrado.</li><li>- Capacidad de Inspección SSL.</li></ul></li></ul>
Networking	<p>La solución garantiza y soporta las siguientes especificaciones de acuerdo al datasheet:</p> <ul style="list-style-type: none"><li>• Latencia de Firewall: 4.78 us</li><li>• Nuevas sesiones por segundo (TCP): 280.000</li><li>• Seguridad: protección avanzada contra malware</li><li>• Rendimiento para IPv4/IPv6, Vlan</li><li>• DHCP Cliente y Servidor DHCP</li><li>• Políticas de enrutamiento</li><li>• NAT</li><li>• Enrutamiento dinámico</li><li>• Soporte: 500 Túneles VPN SSL</li><li>• La solución de Firewall ofertada debe ser capaz de realizar Backup/Restore de la configuración</li><li>• La solución ofertada deberá tener un módulo dedicado para almacenar y autenticar claves criptográficas para protección de ataques maliciosos y ataques de phishing.</li></ul>
Desempeño por Gateway	<p>Debe tener IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) mínima de 27 / 27 / 11 Gbps</p> <p>Debe soportar al menos 3 Millones de Sesiones Concurrente (TCP).</p> <p>Debe soportar al menos 13 Gbps de Throughput de VPN IPSec.</p> <p>Debe soportar al menos un Performance de:</p> <ul style="list-style-type: none"><li>- IPS Throughput: 5 Gbps</li><li>- NGFW Throughput: 3.5 Gbps</li><li>- Rendimiento de Protección contra amenazas: 3 Gbps</li></ul> <p>Debe soportar al menos 10.000 de Políticas de Firewall</p> <p>Debe soportar al menos 4 Gbps de SSL Inspection Throughput (IPS, HTTPS).</p>
Informes	Crear reportes que puedan ser programados para ser enviados por correo electrónico de manera automática.



## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

	Servicios de seguridad	El fabricante debe ofrecer a través de Laboratorios distribuidos por todo el mundo, una inteligencia en tiempo real sobre las amenazas, ofreciendo actualizaciones de seguridad completas.
	Soporte	La solución incluye: Soporte, garantía y licenciamiento de fábrica por 3 años a nivel hardware y software en modalidad 24x7. <ul style="list-style-type: none"> <li>Métodos de respuesta: Teléfono/correo electrónico, soporte remoto.</li> <li>Debe contar con un sistema de soporte online provisto por el fabricante.</li> <li>Contar con un sistema de soporte online provisto por el oferente local.</li> <li>Instalación y configuración con las políticas de seguridad que se le entregarán a la empresa adjudicada para la puesta en marcha del equipo.</li> <li>A partir de la recepción, el proveedor adjudicado se compromete a realizar la transferencia de conocimientos a dos funcionarios del Departamento de TIC's, con objeto de conseguir la información completa de la instalación, administración, configuración, operatividad y manejo de la solución Firewall ofertada, por el tiempo de al menos 8 horas y entregará un certificado de capacitación avalado por el profesional especialista en seguridad informática experimentado en la administración del equipo ofertado. (La capacitación será en las instalaciones del SCPN).</li> </ul>
<b>1</b> <b>SWITCH DE ACCESO SG220-50P 50-PORT GIGABIT POE, INCLUYE 2 TRANSCEIVER GIGABIT ETHERNET MGBSX1</b>	Modelo	Equipo: Switch Cisco SG220-50P 50-Port Gigabit POE incluye 2 transceiver Gigabit Ethernet MGBSX1. El modelo de switch es nuevo de fábrica, no remanufacturado, no debe tener "End of Sale" (Fin de venta) ni "End of Support" (Fin de soporte) anunciado por el fabricante, o por discontinuarse en los próximos 12 meses. Así como también deberá garantizar la disponibilidad de partes y piezas, acceso a actualizaciones de firmware y versiones, parches para el tiempo de duración del contrato.
	Rendimiento	<ul style="list-style-type: none"> <li>Debe contar con memoria de CPU de 128 MB o superior.</li> <li>Debe soportar una memoria flash de 32 MB o superior.</li> <li>Debe soportar al menos una tasa de retransmisión expresada en millones de paquetes por segundo (mpps; basada en paquetes de 64 bytes): 74,40</li> </ul>
	Switching de capa 2	<p>Debe soportar un máximo de 256 VLAN activas simultáneas. VLAN basadas en puertos y en etiquetas 802.1Q Gestión de VLAN</p> <p>Debe tener compatibilidad con el protocolo de árbol de extensión 802.1d estándar.</p>
	Seguridad	Debe soportar Listas de control de acceso (ACL) de hasta 512 reglas.
		Debe tener capacidad de bloquear direcciones MAC de origen a los puertos y limitar el número de direcciones MAC detectadas.
		Debe contar con la funcionalidad de prevención de ataques de denegación de servicio DoS.
	Características de Red	Debe ser compatible con filtrado de dirección MAC.
		Debe contar con protección de sesiones de administración mediante RADIUS y TACACS+, y compatibilidad con autenticación local de bases de datos, así como con sesiones de administración segura a través de SSL, SSH y SNMP v3.
	Administración	<p>El equipo cuenta con las siguientes características de red mínimas:</p> <ul style="list-style-type: none"> <li>48 puertos 10/100/1000 PoE con 375 W de presupuesto energético.</li> <li>2 puertos combinados Gigabit RJ45/SFP</li> <li>Compatibilidad con Power over Ethernet 802.3 af, 802.3 at.</li> <li>INCLUYE 2 TRANSCEIVER GIGABIT ETHERNET para Fibra Multimodo de distancia máxima 550 m (MGBSX1) (Los módulos deben ser de última generación, nuevos de fábrica, no remanufacturados (no refurbished), ni reparados, ni reacondicionados en ninguna de sus partes o componentes.), compatible con el Switch ofertado.</li> </ul> <p>El equipo cuenta mínimo con:</p> <ul style="list-style-type: none"> <li>Administración remota</li> <li>Interfaz de línea de comandos (CLI).</li> <li>Interfaz de usuario web.</li> <li>Soportar SNMP versiones 1.2c y 3.</li> <li>Coexistencia de ambas pilas de protocolos para facilitar la migración de IPv4/IPv6.</li> <li>Soportar QoS.</li> <li>Compatibilidad con telefonía IP.</li> </ul>
	Soporte	La solución incluye: Soporte y garantía por 3 años. El equipo debe contar con soporte del fabricante para actualizaciones de seguridad todo el tiempo de duración de la garantía del equipo.

### 3. CONDICIONES OPERATIVAS

Dando cumplimiento al detalle del Contrato N° SCPN-AJ-026-2021 del proceso “**ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN**”, se pone en conocimiento que se ha recibido lo detallado en el ítem 2, conjuntamente la Administradora del Contrato y el Técnico miembro de la comisión de recepción designados mediante oficio Nro. SCPN-CP-113-2021 de fecha 09 de julio de 2021, en tal razón nos permitimos indicar las actividades realizadas en conjunto con el personal técnico designado de la empresa adjudicada GREENDC S.A.:

- Con fecha 05 de agosto de 2021 el proveedor adjudicado GREENDC S.A., procedió a entregar los siguientes equipos informáticos objeto de este contrato, los mismos que fueron recibidos por la Administradora del Contrato y el Técnico miembro de la comisión de recepción:

Descripción	Marca	Modelo	Color	Serie
<b>Equipo de Seguridad Firewall</b>	Fortinet	FG-200F	Blanco	FG200FT921902015
<b>Switch de acceso</b>	Cisco	SG-220-50P	Gris	DNI2522044K

- Con fecha 11 de agosto de 2021 mediante oficio Nro. SCPN-TIC-AR-039-2021 se solicitó el ingreso provisional a Bodega el proveedor adjudicado GREENDC S.A., procedió a entregar los siguientes equipos informáticos objeto de este contrato, los mismos que fueron recibidos por la Administradora del Contrato y el Técnico miembro de la comisión de recepción:
- Con fecha 13 de agosto de 2021 se recibe el memorando Nro. SCPN-DA-281-2021, suscrito por la señorita Subteniente de Policía Lezlie Romero Anchatipán, Jefe Administrativo Subrogante, en el cual remite el ingreso provisional a bodega Nro. 2021-13.
- Con fecha 14 de agosto de 2021 se coordinó con el personal técnico del proveedor adjudicado GREENDC S.A., para la instalación, configuración, puesta en marcha del nuevo equipo Firewall Fortinet 200F y capacitación, a continuación se detalla las actividades realizadas:

#### 1. Creación de cuenta en Fortinet

Para el registro del equipo, se utilizó una cuenta en Fortinet: <https://support.fortinet.com>, el correo utilizado para dicha cuenta, es la cuenta de correo electrónico: [sistemas@cesantiapn.com.ec](mailto:sistemas@cesantiapn.com.ec), con la que se procedió a registrar el contrato de soporte y equipo.

Las licencias de los servicios de Fortiguard expiran con fecha 14 de Agosto del 2024 como se puede observar en la figura 1:



## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

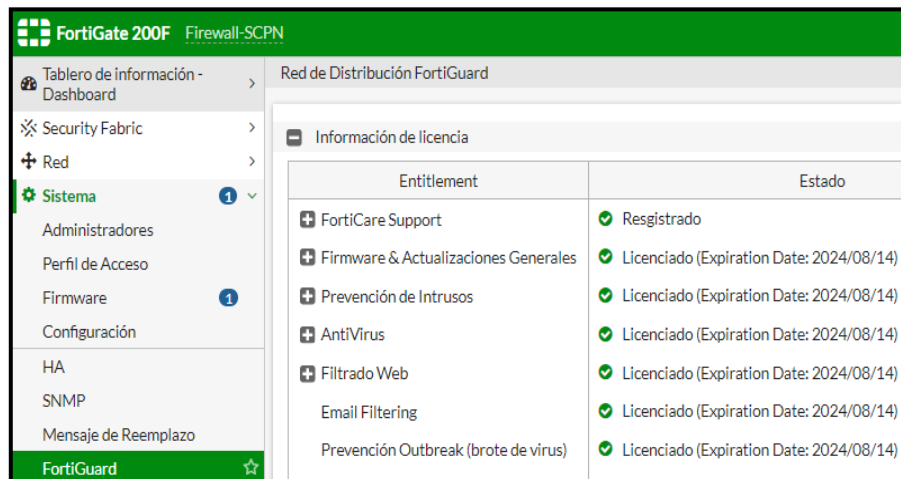


Figura 1. Activación de licenciamiento y soporte

## 2. Usuarios de Administración

Para la autenticación de administración del equipo Fortinet 200F se utiliza la base de datos interna del Fortigate, se tiene tres cuentas para administrar el dispositivo, con los siguientes usuarios: admin, vayala y wortizg como se indica en la figura 2:

Administrador de sistema				
admin		super_admin	Local	Deshabilitado
vayalay	192.168.1.198/32	super_admin	Local	Deshabilitado
wortizg	192.168.1.196/32	super_admin	Local	Deshabilitado

Figura 2. Usuarios de administración

## 3. Configuración de interfaz WAN

A continuación, en la figura 3 se indica la configuración de la interfaz WAN del equipo Fortinet la cual se encuentra conectada mediante el puerto 7 hacia el router del proveedor de internet, mediante la IP Pública 181.198.14.18 con máscara: 255.255.255.240.

Interfaz Física					
CNT (port8)	Interfaz Física		186.47.101.74/255.255.255.248		PING HTTPS SNMP FMG-Access
ha	Interfaz Física		0.0.0.0/0.0.0.0		
LINKNET360 (port7)	Interfaz Física		181.198.14.18/255.255.255.240		PING HTTPS SNMP FMG-Access

Figura 3. Configuración interfaz WAN

#### **4. Configuración de interfaz LAN**

En la siguiente figura 4 se indica la configuración en un interfaz en el puerto 1, para los usuarios de la LAN de las distintas redes que utiliza el SCPN, con dirección IP: 192.168.3.74/29, y la configuración para la interfaz en el puerto 3 para el enlace MPLS, con la dirección IP: 172.24.0.234/29 conectado mediante enlace dedicado hacia Banco Central del Ecuador.

Hardware Switch 2					
lan	Hardware Switch	port1	192.168.3.74/255.255.255.248		PING HTTPS SSH HTTP FMG-Access
MPLS	Hardware Switch	port3	172.24.0.234/255.255.255.248		PING HTTPS HTTP

Figura 4. Configuración interfaz LAN y MPLS

#### **5. Configuración de rutas estáticas.**

Para establecer la conexión hacia internet, red de Banco Central y red de Guayaquil se configuran las siguientes rutas estáticas, como se observa en la figura 5:

FortiGate 200F Firewall-SCPN					
<div> <div> <div>Tablero de información - Dashboard</div> <div>Security Fabric</div> <div>Red</div> <div>Interfaces</div> <div>DNS</div> <div>Captura de paquetes</div> <div>Zonas SD-WAN</div> <div>Reglas SD-WAN</div> <div>Chequeo de estado SD-WAN</div> <div>Static Routes</div> </div> <div> <div>+ Crear nuevo</div> <div>Editar</div> <div>Clonar</div> <div>Borrar</div> <div>Buscar</div> </div> </div>					
Destino	IP de puerta de enlace	Interface	Estatus	Comentarios	
IPv4					
192.168.254.0/25	172.24.0.233	MPLS	Habilitado		
192.168.0.0/22	192.168.3.73	lan	Habilitado		
0.0.0.0/0	181.198.14.17	LINKNET360 (port7)	Habilitado		
192.168.10.0/24	192.168.0.7	lan	Habilitado	ENLACE GUAYAQUIL	

Figura 5. Configuración ruta estáticas

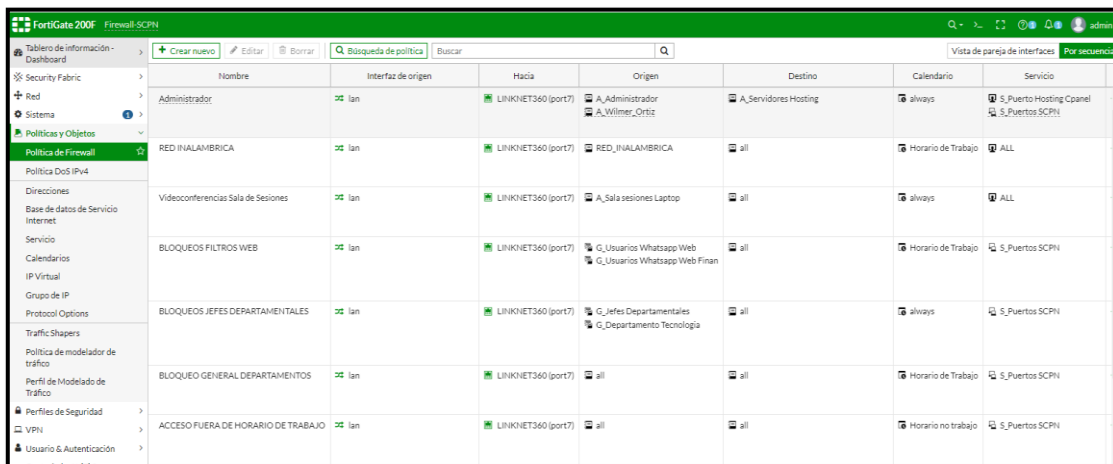
- La primera ruta estática permite la conexión desde la LAN del SCPN hacia la red de Banco Central del Ecuador (Casa de la Moneda) conectado mediante un enlace dedicado.
- La segunda ruta estática permite la conexión de las subredes de la LAN del SCPN.
- La tercer ruta estática permite la conexión de internet por la interfaz WAN del proveedor del servicio LINKNET.
- La cuarta ruta estática permite la conexión hacia la red de Guayaquil a través de un enlace dedicado, conectado al switch de Core del SCPN.

#### **6. Configuración de políticas de seguridad IPv4 para navegación de internet.**

En la figura 6, se procedió a crear políticas de seguridad para navegación de usuarios mediante la creación de perfiles para navegación; BLOQUEO FILTROS WEB, BLOQUEOS JEFES

DEPARTAMENTALES, BLOQUEO GENERAL DEPARTAMENTOS Y ACCESO FUERA DE HORARIO DE TRABAJO.

La política de navegación de BLOQUEO GENERAL DEPARTAMENTOS y ACCESO FUERA DE HORARIO DE TRABAJO, tiene establecido un horario para que trabaje la política en horarios de oficina y entre otra política en funcionamiento sin restricciones en otro horario.

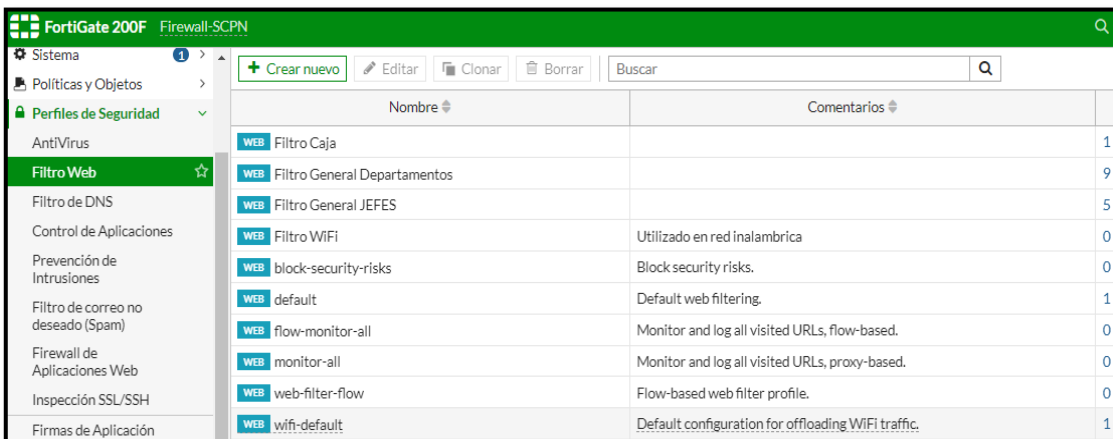


Nombre	Interfaz de origen	Hacia	Origen	Destino	Calendario	Servicio
Administrador	lan	LINKNET360 (port7)	A_Administrador A_Wilmer_Ortiz	A_Servidores Hosting	always	S_Puerto Hosting Cpanel S_Puertos SCPN
RED INALAMBRICA	lan	LINKNET360 (port7)	RED_INALAMBRICA	all	Horario de Trabajo	ALL
Videoconferencias Sala de Sesiones	lan	LINKNET360 (port7)	A_Sala sesiones Laptop	all	always	ALL
BLOQUEOS FILTROS WEB	lan	LINKNET360 (port7)	G_Usuarios Whatsapp Web G_Usuarios Whatsapp Web Finan	all	Horario de Trabajo	S_Puertos SCPN
BLOQUEOS JEFES DEPARTAMENTALES	lan	LINKNET360 (port7)	G_Jefes Departamentales G_Departamento Tecnologia	all	always	S_Puertos SCPN
BLOQUEO GENERAL DEPARTAMENTOS	lan	LINKNET360 (port7)	all	all	Horario de Trabajo	S_Puertos SCPN
ACCESO FUERA DE HORARIO DE TRABAJO	lan	LINKNET360 (port7)	all	all	Horario no trabajo	S_Puertos SCPN

Figura 6. Configuración de políticas para salida a internet

## 7. Configuración de Perfiles de Navegación

A continuación en la figura 7, se muestran los perfiles de navegación configurados para cada una de las políticas IPV4:



Nombre	Comentarios	
WEB Filtro Caja		1
WEB Filtro General Departamentos		9
WEB Filtro General JEFES		5
WEB Filtro WIFI	Utilizado en red inalamblica	0
WEB block-security-risks	Block security risks.	0
WEB default	Default web filtering.	1
WEB flow-monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB monitor-all	Monitor and log all visited URLs, proxy-based.	0
WEB web-filter-flow	Flow-based web filter profile.	0
WEB wifi-default	Default configuration for offloading WIFI traffic.	1

Figura 7. Configuración de perfiles de navegación

## 8. Configuración de Perfiles DNS

Para el control de navegación de solicitudes de C&C y Botnets, se utiliza el perfil default y se habilita el perfil DNS en todas las políticas de navegación, como se indica en la figura 8:



## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

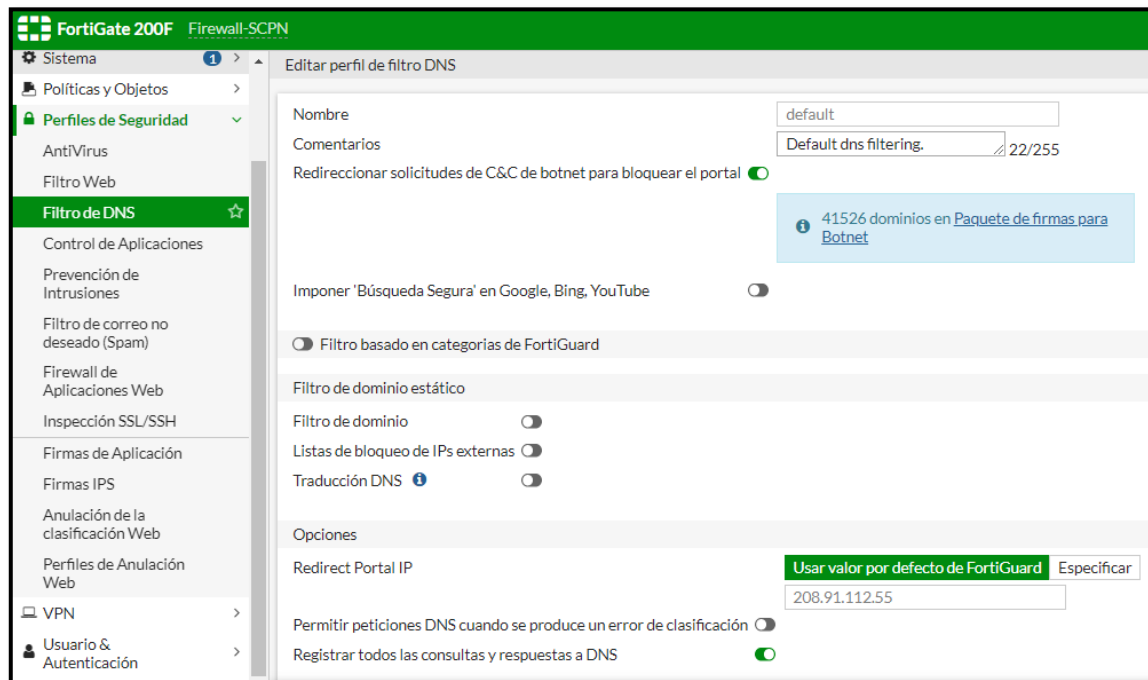


Figura 8. Configuración de perfiles DNS

### 9. Configuración de Perfiles de Antivirus

Para el control de antivirus se configura el perfil defaultantivirus2. A continuación, en la figura 9, se muestra el perfil de antivirus configurado para ser usados en la políticas IPV4:

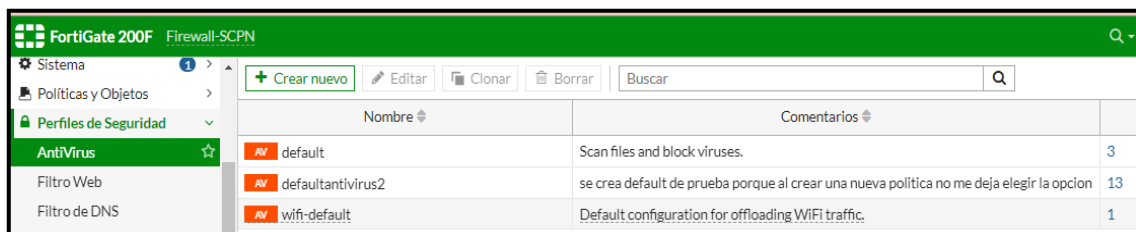


Figura 9. Configuración de perfiles Antivirus

### 10. Configuración de Políticas IPv4

Para poder publicar servicios a través de las IPs públicas se configura el tráfico desde Internet (puerto 7) a la red LAN (puerto 1), se tiene configurado políticas actualmente de varias aplicaciones, como se puede observar en la siguiente figura 10:

Nombre	Interfaz de origen	Hacia	Origen	Destino	Calendario	Servicio	Acción
ACCESO EXTERNO SERV ATLAS PRUEBAS	LINKNET360 (port7)	lan	all	V_Servidor de Pruebas V_Servidor de Pruebas Seguro	always	S_Puertos Enlaces Externos	ACEPTAR
Gestor Documental	LINKNET360 (port7)	lan	all	V_Servidor Documental	always	S_Puertos Enlaces Externos	ACEPTAR
ACCESO EXTERNO APP MANTIS	LINKNET360 (port7)	lan	all	V_Aplicacion Mantis Seguro V_Aplicacion Mantis V_Aplicacion Soporte Mantis	always	S_Puertos SCPN	ACEPTAR
ATLAS CONVENIOS	LINKNET360 (port7)	lan	all	V_Servidor Atlas Convenios V_Servidor Atlas Convenios Seguro	always	S_Puertos Enlaces Externos	ACEPTAR
ACCESO A SERVIDOR DE APP ATLAS	LINKNET360 (port7)	lan	all	V_Servidor de Aplicaciones Atlas V_Servidor de Aplicaciones Atlas ...	always	S_Puertos Enlaces Externos	ACEPTAR

Figura 10. Configuración de políticas IPv4

## 11. Configuración de NAT

Para la publicación de aplicaciones del SCPN en internet se realizan las siguientes configuraciones de IP Virtuales, como se indica en la figura 11:

Nombre	Detalles	Interfaces
IP Virtual IPv4 13		
V_Servidor de Aplicaciones Atlas	181.198.14.21 → 192.168.0.194 (TCP: 80 → 80)	LINKNET360 (port7)
V_Servidor de Aplicaciones Atlas Seguro	181.198.14.21 → 192.168.0.194 (TCP: 443 → 443)	LINKNET360 (port7)
V_Servidor de Pruebas Seguro	181.198.14.22 → 192.168.0.196 (TCP: 443 → 443)	LINKNET360 (port7)
V_Servidor de Pruebas	181.198.14.22 → 192.168.0.196 (TCP: 80 → 80)	LINKNET360 (port7)
V_Aplicacion Mantis Seguro	181.198.14.23 → 192.168.0.3 (TCP: 443 → 443)	LINKNET360 (port7)
V_Aplicacion Mantis	181.198.14.23 → 192.168.0.3 (TCP: 80 → 80)	LINKNET360 (port7)
V_Aplicacion Soporte Mantis	181.198.14.23 → 192.168.0.3 (TCP: 7777 → 7777)	LINKNET360 (port7)
V_Servidor Documental	181.198.14.24 → 192.168.0.197 (TCP: 80 → 80)	LINKNET360 (port7)
V_Aplicacion Turnos en Línea SCPN	181.198.14.19 → 192.168.0.9 (TCP: 443 → 443)	LINKNET360 (port7)
V_Aplicacion Turnos en Línea	181.198.14.19 → 192.168.0.9 (TCP: 80 → 80)	LINKNET360 (port7)
V_Aplicacion Turnos en Línea 1	181.198.14.19 → 192.168.0.9 (TCP: 8080 → 8080)	LINKNET360 (port7)
V_Servidor Atlas Convenios	181.198.14.20 → 192.168.0.193 (TCP: 80 → 80)	LINKNET360 (port7)
V_Servidor Atlas Convenios Seguro	181.198.14.20 → 192.168.0.193 (TCP: 443 → 443)	LINKNET360 (port7)

Figura 11. Configuración de políticas IPv4

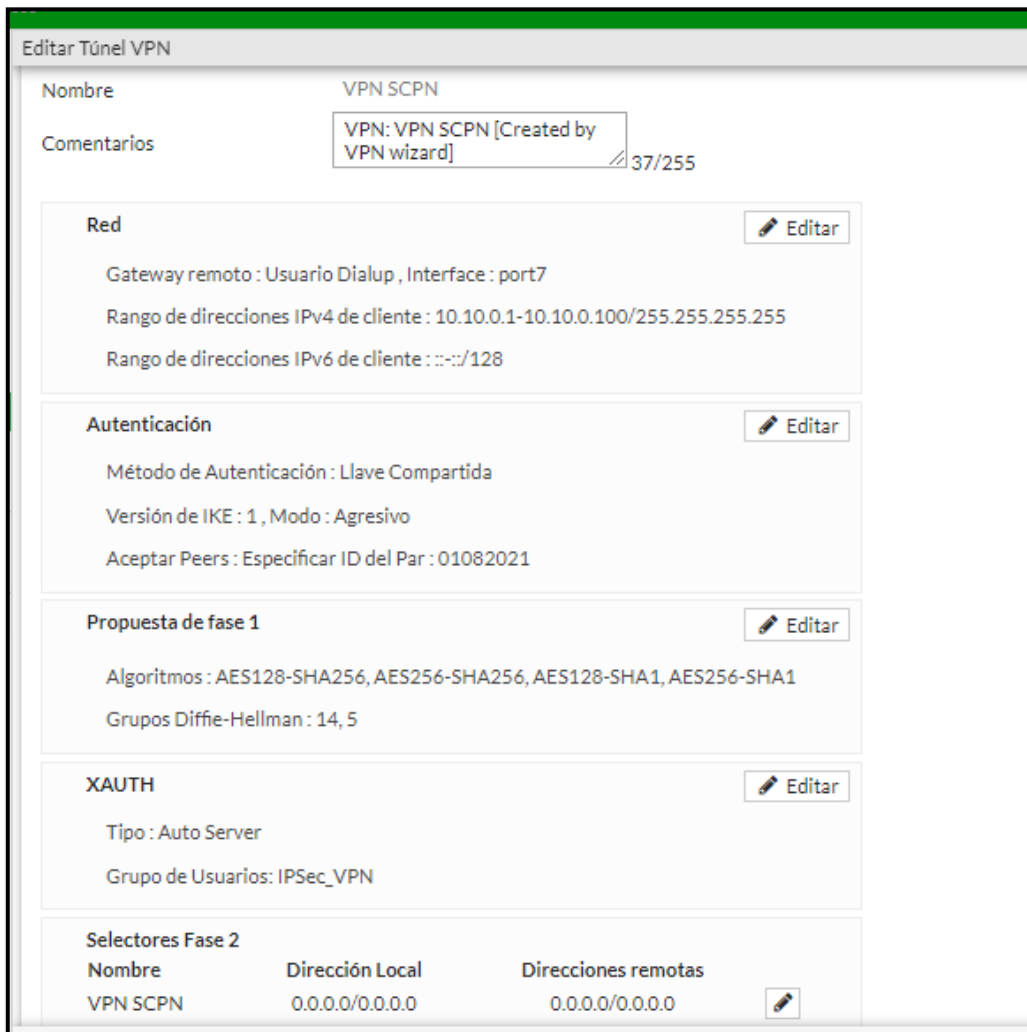
## 12. Configuración de políticas para una VPN (Red Privada Virtual) IPsec

En la siguiente figura 12 se puede observar la configuración de un túnel VPN IPsec, el rango de direcciones que se puede asignar en el túnel ipsec de acuerdo con lo que se puede observar en la configuración es de la ip 10.10.0.1 a la ip 10.10.0.100. El grupo de usuarios para establecer la conexión del túnel Ipsec es IPsec\_VPN.

Se ha configurado una llave compartida para el acceso VPN, la misma que puede ser cambiada en caso de que no se tenga acceso, desde la configuración del túnel Ipsec.

Con el propósito de que se puedan configurar distintos perfiles de VPN IPsec y generar distintos perfiles para el acceso a ciertas redes de SCPN, se coloca un LOCALID: 01082021.





**Editar Túnel VPN**

Nombre: VPN SCPN

Comentarios: VPN: VPN SCPN [Created by VPN wizard] 37/255

**Red** [Editar]

Gateway remoto: Usuario Dialup, Interface: port7

Rango de direcciones IPv4 de cliente: 10.10.0.1-10.10.0.100/255.255.255.255

Rango de direcciones IPv6 de cliente: :::/128

**Autenticación** [Editar]

Método de Autenticación: Llave Compartida

Versión de IKE: 1, Modo: Agresivo

Aceptar Peers: Especificar ID del Par: 01082021

**Propuesta de fase 1** [Editar]

Algoritmos: AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1

Grupos Diffie-Hellman: 14, 5

**XAUTH** [Editar]

Tipo: Auto Server

Grupo de Usuarios: IPSec\_VPN

**Selectores Fase 2**

Nombre	Dirección Local	Direcciones remotas
VPN SCPN	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Figura 12. Configuración de VPN IPSec

Para establecer la conexión de dispositivos remotos, se configura un perfil de VPN IPSec. Dentro de los túneles IPSec como se puede observar se tiene configurado un tipo de túnel Ipsec, como se puede observar en la siguiente figura 13:

Túnel	Enlace de Interface	Estado	Referencia
Personalizar 1			
VPN SCPN	LINKNET360(port7)	1 conexión(es) dialup	3

Figura 13. Configuración de VPN IPSec

### 13. Configuración de políticas IPV4 de VPN IPSec

Para la comunicación de la red LAN (puerto 1), Internet (puerto 7) y la VPN SCPN, con los usuarios remotos que se conecten por VPN IPSec, se configuran las siguientes políticas IPV4, como se puede observar en la figura 14 que se presenta a continuación:



vpn_VPN SCPN_remote_0	VPN SCPN_range	LAN_TIC LAN_VPN LAN_ENLACE	always	ALL	ACEPTAR	Habilitado	SSL no-inspection	UTM	1.42 GB
VPN SCPN INTERNET	VPN SCPN_range	all	always	ALL	ACEPTAR	Habilitado	SSL no-inspection	UTM	6.33 GB

Figura 14. Configuración de IPv4 para VPN IPsec

Para la red para la comunicación con las redes LAN de SCPN que se desee dar acceso y para que los usuarios que se conecten a la VPN IPSEC remota puedan tener acceso a internet a través del puerto 7.

#### **14. Configuración de VPN (Red Privada Virtual) IPsec en FortiClient:**

En la figura 15, se indica la configuración de VPN IPsec en la aplicación Forticlient la cual utilizan los usuarios para conexión remota hacia la red del SCPN.



FortiClient -- The Security Fabric Agent

File Help

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

**Editar Conexión VPN**

VPN: VPN SSL VPN IPsec XML

Nombre de Conexión:

Descripción:

Gateway Remoto:  ✕  
[+Adicionar Gateway Remoto](#)

Método de Autenticación: Clave pre-compartida

Autenticación (XAuth): ☐ Preguntar en el login ☒ Guardar login ☐ Deshabilitar

Nombre de Usuario:

Figura 15. Configuración de VPN IPsec en FortiClient

En ajustes avanzados, unicamente se debe revisar el LOCAL ID:



— Ajustes avanzados

+ Configuración de VPN

— Fase 1

**Propuesta IKE**

Encriptación: AES128 Autenticación: SHA1

Encriptación: AES256 Autenticación: SHA256

**Grupo DH**

☐ 1 ☐ 2 ☒ 5 ☐ 14 ☐ 15

☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20

**Vida de Clave**

seg

**ID Local**

☒ Detección de Par Muerto (DPD)

☒ NAT Transversal

Figura 16. Configuración de VPN IPsec en FortiClient (1)

### 15. Configuración de reportes

Para la generación de reportes en Forticloud esta creada la cuenta sistemas@cesantiapn.com.ec, Forticloud es un servicio en nube donde se puede almacenar los logs del equipo Fortigate por 7 días. La cuenta Forticloud es versión Free por lo que únicamente se pueden almacenar y generar informes por el tiempo de 7 días. En caso de que se desee almacenar los logs por más tiempo se debería actualizar la licencia para almacenamiento en nube a una que sea en modalidad pago.

Se generarán dos reportes, en la cuenta de Forticloud, que se enviarán semanalmente a la cuenta de correo: alertas@cesantiapn.com.ec, como se puede observar en la siguiente gráfica 17:

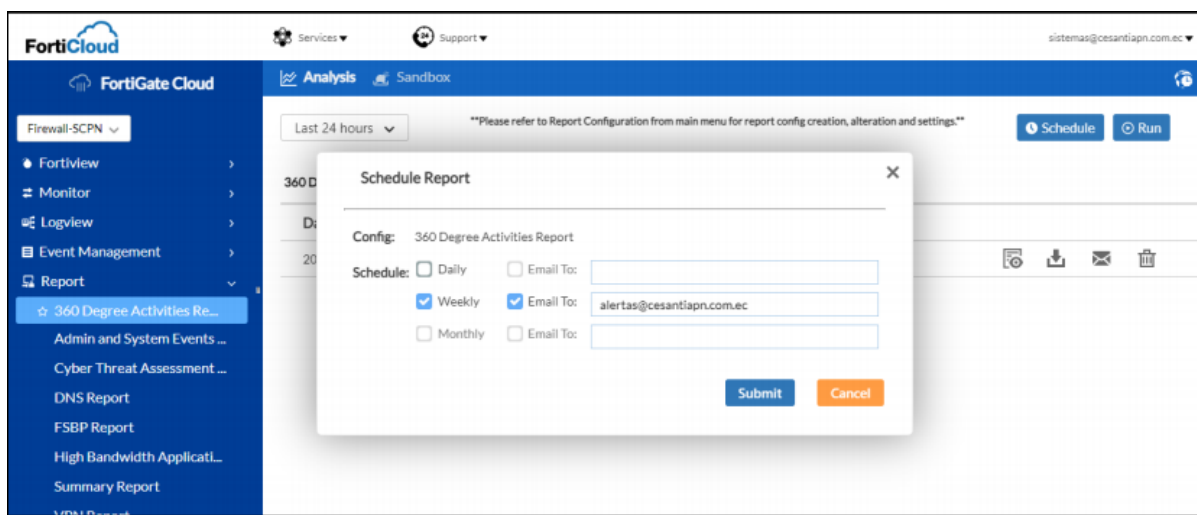


Figura 17. Configuración de reportes en Forticloud

### 16. Pruebas de conectividad

- En la figura 18 se puede observar una prueba de verificación de conexión desde la red SCPN Quito hacia la red SCPN Guayaquil, en la cual no existe pérdida de paquetes.

```

Consola CLI (2)
Firewall-SCPN # execute ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: icmp_seq=0 ttl=248 time=39.8 ms
64 bytes from 192.168.10.1: icmp_seq=1 ttl=248 time=21.0 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=248 time=26.4 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=248 time=44.2 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=248 time=42.5 ms

--- 192.168.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 21.0/34.7/44.2 ms
    
```

Figura 18. Prueba de conexión desde red SCPN Quito hacia red SCPN Guayaquil

## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

- En la figura 19 se puede observar una prueba de verificación de conexión desde la red SCPN Quito hacia la red de Banco Central del Ecuador (Casa de la Moneda), en la cual no existe pérdida de paquetes.

```

Consola CLI (2)

Firewall-SCPN # execute ping 192.168.254.50
PING 192.168.254.50 (192.168.254.50): 56 data bytes
64 bytes from 192.168.254.50: icmp_seq=0 ttl=250 time=15.2 ms
64 bytes from 192.168.254.50: icmp_seq=1 ttl=250 time=6.3 ms
64 bytes from 192.168.254.50: icmp_seq=2 ttl=250 time=2.4 ms
64 bytes from 192.168.254.50: icmp_seq=3 ttl=250 time=2.0 ms
64 bytes from 192.168.254.50: icmp_seq=4 ttl=250 time=1.8 ms

--- 192.168.254.50 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.8/5.5/15.2 ms
  
```

Figura 19. Prueba de conexión desde red SCPN Quito hacia red BCE

- En la figura 20 se puede observar una prueba de verificación de conexión desde el Fortinet 200F hacia la LAN SCPN Quito, en la cual no existe pérdida de paquetes.

```

Consola CLI (1)

Firewall-SCPN # execute ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10): 56 data bytes
64 bytes from 192.168.0.10: icmp_seq=0 ttl=127 time=0.2 ms
64 bytes from 192.168.0.10: icmp_seq=1 ttl=127 time=0.1 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=127 time=0.1 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=127 time=0.1 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=127 time=0.1 ms

--- 192.168.0.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
  
```

Figura 20. Prueba de conexión de subredes

#### 17. Verificación de activación de soporte para el switch de acceso cisco SG220

Dentro de la adquisición, se recibió a satisfacción el switch Cisco SG220-50P, con el soporte de fábrica activado hasta la fecha: 13 de Agosto del 2024, como se puede observar en la figura 21:

Offer/Product Name	Contract Number/ Subscription ID	Start Date / End Date	End Customer	Service Level / Offer Type
SG220-50P-K9-NA SG220-50P 50-Port Gigabit PoE S...	204303839 ACTIVE	14-Aug-2021 13-Aug-2024	SERVICIO DE CESAN... (1022365706), EC	SNT SNTC 8X5XNBD CON-SNT-G2059NA2

Figura 21. Activación de soporte de switch cisco SG220

## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

#### 4. LIQUIDACIÓN ECONÓMICA:

De acuerdo al contrato Nro. SCPN-AJ-026-2021 en su parte pertinente indica;

- “Cláusula Quinta.- **FORMA DE PAGO.** Se pagará al oferente el 100% contra entrega de los productos, previa firma del acta de entrega recepción definitiva de los equipos, entrega de garantías correspondientes, presentación de la factura e informe de satisfacción del administrador del contrato.”

Una vez que se ha recibido los bienes a satisfacción, la liquidación económica del contrato Nro. SCPN-AJ-026-2021, del pago total es de USD 17.500,00 (Diecisiete mil quinientos con 00/100 dólares de los Estados Unidos de América), más IVA como se indica en la siguiente tabla:

Ítem	Especificación	Cantidad	Valor sin iva	Valor con iva Total	Estado
1	ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN	1	17.500,00	19.600,00	Valor Total Contratado
2	FIREWALL NGFW FORTINET 200F	1	15.759,00	17.650,08	Valor Pendiente de pago
3	SWITCH CISCO SG220-50P 50-PORT GIGABIT POE, INCLUYE 2 TRANSCEIVER GIGABIT ETHERNET MGBSX1	1	1.741,00	1.949,92	
<b>Saldo por devengar del Contrato</b>			<b>17.500,00</b>	<b>19.600,00</b>	

#### 5. LIQUIDACIÓN DE PLAZOS

De acuerdo a lo establecido en el contrato Nro. SCPN-AJ-026-2021 y la entrega de los bienes esperados, la liquidación de plazos es la siguiente:

Nº	DESCRIPCIÓN	FECHAS
1	Firma de Contrato: SCPN-AJ-026-2021	09/07/2021
2	El proveedor adjudicado GREENDC S.A., entrega los equipos informáticos	05/08/2021
3	Puesta en marcha del equipo de seguridad Firewall Fortinet 200F	14/08/2021
4	<b>Finalización de la contratación</b>	<b>23/08/2022</b>

##### 5.1.MULTAS

De conformidad con la orden de compra, se considera que no se aplican multas ya que la entrega del producto estuvo enmarcada dentro de los plazos contractuales.

#### 6. CONSTANCIA DE LA RECEPCIÓN

Dando cumplimiento al contrato Nro. SCPN-AJ-026-2021 del objeto “**ADQUISICIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PARA EL SCPN**” de fecha 09 de julio de 2021. después de haber constatado, revisado y comparado el trabajo realizado por la empresa GREENDC S.A., representada por el señor Ing. Ruben Xavier Suquillo Armas con número de RUC 1792422426001, y los términos

## SERVICIO DE CESANTÍA DE LA POLICÍA NACIONAL

### DEPARTAMENTO DE TECNOLOGÍA

de referencia para la contratación se puede establecer que los equipos informáticos se encuentran a entera satisfacción del Servicio de Cesantía de la Policía Nacional.

#### 7. CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES

El proveedor adjudicado GREENDC S.A., entregó un informe técnico que ha sido revisado por el señor Ing. Raul Alejandro Rodriguez Parra como Técnico miembro de la comisión de recepción, por lo que se concluye técnicamente que cumple a cabalidad con lo establecido en lo referido a la contratación y se da por finalizado el contrato Nro. SCPN-AJ-026-2021 de acuerdo al plazo de ejecución.

#### 8. REAJUSTES DE PRECIOS PAGADOS Y/O PENDIENTES DE PAGO

De conformidad con el contrato, se considera que no se aplica reajuste de precios ya que la entrega de los bienes esperados estuvo enmarcada dentro de los valores contractuales.

#### 9. ACEPTACIÓN DE LAS PARTES

Para constancia de lo actuado y de conformidad con lo expresado, firman al pie del presente, los señores miembros de la comisión de entrega-recepción, y el contratista.

D.M. de Quito, 27 de agosto del 2021.

#### COMISIÓN DE ENTREGA RECEPCIÓN Y PROVEEDOR ADJUDICADO

 <p>Firmado electrónicamente por: <b>VIVIANA ELIZABETH AYALA YANDUN</b></p>	 <p>Firmado electrónicamente por: <b>RAUL ALEJANDRO RODRIGUEZ PARRA</b></p>	 <p>Firmado electrónicamente por: <b>RUBEN XAVIER SUQUILLO ARMAS</b></p>
Ing. Viviana Elizabeth Ayala Yandún	Ing. Raul Alejandro Rodriguez Parra	Ing. Ruben Xavier Suquillo Armas
<b>ADMINISTRADORA DEL CONTRATO (SCPN-AJ-026-2021)</b>	<b>TÉCNICO MIEMBRO DE LA COMISIÓN DE RECEPCIÓN</b>	<b>REPRESENTANTE LEGAL GREENDC S.A.</b>



**GREENDC S.A.**

GREENDC

**Matriz:** AV. OCCIDENTAL N71-282 Y JOSE MIGUEL CARRION

**Teléfono:** 022992900

**Correos:** administracion@greendc.com.ec

**Obligado a Llevar Contabilidad:** Si

Agente de Retención Resolución 1

**R.U.C.:** 1792422426001

**FACTURA**

**No. 001-001-000001405**

**NUMERO DE AUTORIZACIÓN**

1609202101179242242600120010010000014058046010010

**AMBIENTE:** PRODUCCIÓN

**EMISIÓN:** NORMAL

**CLAVE DE ACCESO**



1609202101179242242600120010010000014058046010010

**Información Cliente**

**Cédula/Ruc:** 1768053820001

**Nombre:** SERVICIO DE CESANTIA DE LA POLICIA NACIONAL

**Teléfonos:** 02-395-0900

**Dirección:** 9 DE OCTUBRE N29-24 Y AV. ELOY ALFARO

**Correo:** administracion@greendc.com.ec

**Fecha Emisión:** 16/09/2021

**Fecha Vencimiento:** 16/10/2021

**Vendedor:** STEFANIE MORA

**Moneda:** USD

N	Código	Nombre	Cant.	Precio U.	Desc.	Precio T.
1	VENTA.03	FIREWALL FORTINET FG-200F / BLANCO / S/N: FG200FT921902015	1,00	15.759,00	0,00	15.759,00
2	VENTA.03	SWITCH POE CISCO SG220-50P GRIS S/N: DNI2522044K Incluye 2 transceiver Gigabit Ethernet MGBSX1 S/N: ACW251002Y2 ACW251002Y9	1,00	1.741,00	0,00	1.741,00

Información Adicional		Subtotal	\$ 17.500,00
CONTRATO	SCPN-AJ-026-2021	Subtotal IVA 12%	\$ 17.500,00
Forma de Pago		Subtotal IVA 0%	\$ 0,00
OTROS CON UTILIZACIÓN DEL SISTEMA FINANCIERO		Subtotal No Objeto	\$ 0,00
SON : DIECINUEVE MIL SEISCIENTOS Y 00/100 DÓLARES AMERICANOS		Subtotal Exento	\$ 0,00
		Subtotal Sin Impuestos	\$ 17.500,00
		Descuento	\$ 0,00
		IVA 12%	\$ 2.100,00
		ICE	\$ 0,00
		Servicio	\$ 0,00
		Total	\$ 19.600,00