

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

Anexo No. 1

ESPECIFICACIONES TÉCNICAS MÍNIMAS DEFINITIVAS

OBJETO: Renovar el licenciamiento de acceso y uso de la solución Firewall Checkpoint, incluido soporte técnico especializado, para el Servicio Geológico Colombiano.

El Servicio Geológico Colombiano cuenta actualmente con los siguientes componentes de licenciamiento asociados a la solución de seguridad perimetral, los cuales serán objeto de renovación:

No.	Nombre del bien o servicio	Unidad de medida	Cantidad
1	CPAP-SG9700-PLUS-SNBT – Next Generation Threat Prevention and SandBlast for Quantum Force 9700 Plus Appliance y CPSB-SDWAN-9700-PLUS-1Y – SD-WAN subscription for Quantum Force 9700 Plus Appliance BOGOTÁ	Licencia	2
2	CPAP-SG9400-PLUS-SNBT – Next Generation Threat Prevention and SandBlast for Quantum Force 9400 Plus Appliance y CPSB-SDWAN-9400-PLUS-1Y – SD-WAN subscription for Quantum Force 9400 Plus Appliance PASTO	Licencia	2
3	CPAP-SG1900-SNBT – Next Generation Threat Prevention and SandBlast for Quantum Spark 1900 Appliance y CPSB-SDWAN-1900-1Y – SD-WAN subscription for Quantum Spark 1900 Appliance POPAYÁN, MANIZALES	Licencia	2

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

4	Next Generation Security Management Software for up to 10 Gateways (Agentic Package) – CPSM-NGSM10-COMPLETE	Licencia	1
5	SMOT 1 – Servicios incluidos: Soporte técnico 7x24; Monitoreo de la solución objeto de la renovación; entrega de informes mensuales sobre la gestión y estado de la solución; Realización de un análisis de vulnerabilidades mensualmente durante la vigencia de la licencia sobre la infraestructura relacionada con la solución objeto de renovación, incluyendo el respectivo informe de resultados y recomendaciones de remediación.; Servicios en sitio: Prestación de soporte técnico en sitio cuando sea requerido en las ciudades de Bogotá, Pasto, Popayán y Manizales.	Licencia	1

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

Inventario de Licencias Actuales

Servicio Geologico Fechas		
Producto	SKU	Fechas de vencimiento
Managment VM	CPSB-COMP-5-1Y	17/09/2026
Equipo quantum force 9700	CPAP-SG9700-PLUS-SNBT	20/08/2026
Equipo quantum force 9700	CPAP-SG9700-PLUS-SNBT	20/08/2026
Equipo quantum force 9400	CPAP-SG9400-PLUS-SNBT	20/08/2026
Equipo quantum force 9400	CPAP-SG9400-PLUS-SNBT	20/08/2026
Equipo spark 1900	CPAP-SG1900-SNBT	6/11/2026
Equipo spark 1900	CPAP-SG1900-SNBT	6/11/2026
SD-WAN 9700	CPSB-SDWAN-9700-PLUS-1Y	20/08/2026
SD-WAN 9700	CPSB-SDWAN-9700-PLUS-1Y	20/08/2026
SD-WAN 9400	CPSB-SDWAN-9400-PLUS-1Y	20/08/2026
SD-WAN 9400	CPSB-SDWAN-9400-PLUS-1Y	20/08/2026
SD-WAN 1900	CPSB-SDWAN-1900-1Y	20/08/2026
SD-WAN 1900	CPSB-SDWAN-1900-1Y	20/08/2026

Nota: El licenciamiento y soporte actual de todos los productos mencionados en la tabla anterior, debe tener vigencia hasta el 21 de septiembre de 2027, fecha en la cual todos deben vencer.

Actualmente, la Entidad cuenta con la infraestructura que se detalla a continuación. Para efectos del presente proceso, dicha infraestructura deberá cumplir estrictamente con las siguientes condiciones técnicas:

ITEM	DESCRIPCIÓN
1	REQUERIMIENTOS FIREWALL PRINCIPAL
1.1	El proponente deberá acreditar el cumplimiento de las especificaciones técnicas aplicables a la solución objeto de renovación mediante documentación oficial del fabricante o enlaces a sus sitios web oficiales que permitan verificar las características requeridas por la Entidad.
	Requerimientos Solución de Gestión.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

2.	CONSOLA DE ADMINISTRACION y MONITOREO, LOGS, REPORTES
	Actualmente el Servicio Geológico Colombiano, cuenta con la consola de gestión Check Point Security Manager y consola de reportes Smartreporter, las cuales funcionan en software sobre una solución de hardware virtualizado. La solución debe incluir el software y el licenciamiento necesario requerido para gestionar desde una única consola al menos las siguientes funcionalidades: 1. Firewall (cortafuegos), 2. VPN (Redes privadas virtuales) 3. IPS (Sistema de prevención contra intrusiones) 4. Control de aplicaciones Web 2.0, incluido P2P (Peer to peer - Par to par) 5. Mobile Access unlimited 6. Identificación y control por usuario con utilización de directorio activo 7. Filtrado de URL (Localizador de recursos uniforme) 8. Antivirus 9. Anti-Spam (Anti-Correo Basura), Anti-malware (Anti-Software malicioso) 10. Identity awareness (Control de identidades) 11. Advanced Networking & Clustering (Enrutamiento avanzado y clusterización) 12. Antibot (Anti-Robots) 13. Sandboxing El contratista debe contar con un esquema de mesa de ayuda, que permita el reporte de incidentes, seguimiento, solución y generación de informes de incidentes frente a la prestación del servicio, siguiendo las mejores prácticas de ITIL. El contratista debe entregar informe mensual del estado de la solución, indicando: parámetros de funcionamiento, mejoras, posibles actualizaciones, Monitoreo estado de salud lógico y físico "estado de los nodos, uso de memoria, CPU y almacenamiento". Brechas de seguridad halladas, con su remediación. Reportes

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

	mensuales del estado de la plataforma incluyendo elementos físicos y lógicos. Monitoreo estado de salud hardware (monitoreo remoto de los componentes de hardware “appliances”), tales como: discos, nodos de cómputo y fuentes de poder.		
	SEGMENTO	LICENCIAMIENTO	FUNCIONALIDADES DE SOFTWARE REQUERIDAS
	CONSOLA DE ADMINISTRACIÓN CENTRAL	NEXT GENERATION SECURITY MANAGEMENT SOFTWARE FOR 10 GATEWAYS (WITH AGENTIC PACKAGE FOR 1 YEAR) CPSM-NGSM10-COMPLETE	- ADMINISTRACIÓN CENTRAL, MONITOREO y GESTIÓN DE LAS POLÍTICAS DE SEGURIDAD - LOGS - CORRELACIÓN y REPORTES
2.1	ADMINISTRACIÓN CENTRAL, MONITOREO y GESTIÓN DE LAS POLÍTICAS DE SEGURIDAD		
2.1.1	La solución deberá permitir la administración centralizada de los gateways de seguridad objeto de la renovación.		
2.1.2	La solución debe soportar la gestión de al menos 10 gateways de seguridad red requeridos por la organización.		
2.1.3	La Consola debe permitir administración basada en roles. Debe permitir roles granulares para: acceso de escritura, acceso de lectura, creación de usuarios, delimitar las funciones de configuraciones.		
2.1.4	La administración de la consola de la solución debe soportar acceso por un cliente GUI o vía Web, vía SSH y API abierta.		

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

2.1.5	Debe permitir el acceso de administradores concurrentes; que trabajan a la vez sobre la misma política sin que el trabajo del uno interfiera en el del otro.
2.1.6	La solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
2.1.7	Debe permitir la autenticación integrada con servidor Radius/TACACS.
2.1.8	Debe permitir autenticación de los administradores con proveedor de identidad SAML 2.0.
2.1.9	Permitir enviar los cambios en políticas dentro de un flujo de autorización y escalamiento antes de aplicación.
2.1.10	La solución debe incluir un canal de comunicaciones seguro cifrado entre todos los componentes.
2.1.11	La plataforma de seguridad debe permitir realizar tareas de gestión a través del API.
2.1.12	La solución debe incluir una CA x.509 interno (Autoridad de certificación) que pueda generar certificados para las puertas de enlace y los usuarios para permitir una autenticación fácil.
2.1.13	La solución debe incluir la capacidad de utilizar CA externas, que sea compatible con las normas PKCS # 12, CAPI o Entrust.
2.1.14	La solución debe soportar alta disponibilidad. La consola de administración debe gestionar la solución activo-pasivo.
2.1.15	La solución debe incluir la capacidad de distribuir de forma centralizada y aplicar nuevas versiones de software y/o parches en los gateways de seguridad de red.
2.1.16	La administración de la solución debe posibilitar un conjunto de estadísticas históricas y en tiempo real de los gateways y el tráfico que pasa por los gateways de seguridad: como CPU, Memoria, Disco, Throughput, Conexiones Concurrentes, Conexiones por Segundo.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

2.1.17	Debe posibilitar la integración con soluciones de SIEM del mercado.
2.1.18	La solución debe ofrecer unificación de políticas, esto es en una regla involucrar usuarios, direcciones IP, aplicaciones, tipos de datos, servicios, etc.
2.1.19	La solución es poder unificar objetos IPv4 e IPv6 en una misma regla.
2.1.20	La solución debe incluir la capacidad de administrar centralmente las licencias de todos los gateways de seguridad, incluyendo Firewalls virtualizados Datacenter, Firewall AWS y Firewalls Azure.
2.1.21	Debe permitir instalar paquetes de parches sin conexión a Internet y distribuirlos de forma centralizada.
2.1.22	En caso tal que no se renueve el licenciamiento, la solución siga en funcionamiento para la administración, monitoreo y generación de informes.
	POLÍTICA
2.1.22.1	Debe permitir administrar todas las políticas, reglas y objetos para todos los gateways que componen la plataforma de seguridad, usando una única interfaz de administración.
2.1.22.2	Permitir la creación y administración de políticas de control de acceso (fw, vpn, aplicaciones, url).
2.1.22.3	Permitir la creación y administración de políticas de threat prevention (Anti-virus, Anti-bot, sandboxing).
2.1.23	Debe posibilitar la visualización y comparación de configuraciones actuales y las configuraciones anteriores.
2.1.24	La solución debe permitir revertir la política de seguridad a una versión anterior.
2.1.25	La solución debe informar sobre todas las instalaciones de políticas de seguridad.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

2.1.26	La solución debe soportar creación de múltiples versiones de la política de seguridad de modo que puedan ser consultadas en caso de necesitar revertir algún cambio.
2.1.27	La solución debe permitir configurar e instalar las políticas de prevención de amenazas (IPS, AV, Anti-Bot, Sandbox) de un modo independiente a las políticas de control de acceso (Firewall, Application Control, Url Filtering). Esto para facilitar la administración y favorecer la delegación de funciones.
	OBJETOS
2.1.28	La consola debe permitir la búsqueda de objetos y donde están siendo utilizados: en reglas, gateways, configuraciones, etc.
2.1.29	La solución debe permitir la búsqueda de qué objetos de red contiene una dirección IP específica o parte de ella.
2.1.30	Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificación de los objetos.
	REGLAS
2.1.31	Debe permitir la creación de Reglas que estén activas en un horario definido.
2.1.32	Debe soportar definición de tiempo de expiración a las reglas de seguridad, de modo que estén activas en intervalos específicos de tiempo.
2.1.33	Debe soportar agrupación de reglas en secciones etiquetadas para una administración intuitiva y ordenada.
2.1.34	La solución debe poder compartir y reutilizar un segmento de la base de reglas (por ejemplo, usar el mismo segmento de reglas en diferentes paquetes de políticas).
2.1.35	Debe poder validar errores en las reglas antes de ser instaladas en los gateways de seguridad (ejemplo: cuando haya reglas que oculten o tengan conflicto con otras reglas).
2.1.36	Debe tener contador de utilización (hits) en las reglas de seguridad, para saber que tanto se utilizan las reglas.
2.1.37	La plataforma de seguridad debe permitir a través de API (Application Program Interface) interactuar en tiempo real con la solución permitiendo así que Reglas y políticas de seguridad puedan ser modificadas por un tercero o permitir la integración por API con terceros.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

2.1.38	La solución debe permitir la búsqueda por paquete, es decir, sin necesidad de tener un log asociado a una regla, pueda retornar las reglas que harían match con un tráfico específico.
2.1.39	Por cada coincidencia de una regla, se debe poder configurar alguna de las siguientes opciones: Log, Alert, Send and SNMP trap, send and email, o ejecutar un user defined script.
2.1.40	La solución debe incluir la opción de segmentar la base de reglas usando etiquetas o secciones para mejor organización de la política.
CAPAS	
2.2.1	La solución debe ser capaz de segmentar la política en un conjunto de reglas (capa) en la que solo el tráfico relevante sea inspeccionado por esa capa.
2.2.2	La solución debe ser capaz de segmentar en un conjunto de reglas (capa) en favor de la delegación de funciones para que los cambios en esta capa no afecten a otros segmentos.
2.2.3	La solución debe ser capaz de segmentar en un conjunto de reglas (capa) en favor habilitar una o más funcionalidades de seguridad que no afecten a otros segmentos.
2.3	LOGS
2.3.1	Debe consolidar los logs de tráfico y auditoría de todos los gateways administrados.
2.3.2	Los logs deben ser transferidos con seguridad entre el cluster de Gateway de Seguridad y el servidor de administración.
2.3.3	Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó y el horario del cambio.
2.3.4	El Visor de logs debe tener la capacidad de ver todos los logs de seguridad (firewall, vpn, IPS, control de aplicaciones, filtrado url, antivirus, anti bot) en un panel de visualización.
2.3.5	El Visor de logs debe tener la capacidad de crear un filtro utilizando los objetos predefinidos (hosts, red, grupos, usuarios, etc).
2.3.6	El visor de logs debe tener una función de búsqueda de texto libre.
2.3.7	El Visor de logs debe permitir generar estadísticas (tops) de logs por orígenes, destinos, servicios, protocolos, usuarios, etc.
2.3.8	Debe permitir configurar el tamaño del archivo para rotación de los archivos de logs.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

2.3.9	Debe poderse realizar un respaldo automático de logs, basados en programaciones de tiempo o del tamaño del archivo.
2.3.10	Debe ser posible exportar logs en formato CSV.
2.3.11	Los administradores pueden instalar servidores de logs dedicados para mayor escalabilidad.
2.3.12	La ventana de configuración de reglas debe incluir una sección con el historial detallado para cada regla que incluya información de quien ha modificado la regla.
2.4	CORRELACIÓN Y REPORTES
2.4.1	La solución debe tener una personalización completa de las vistas de resumen y la generación de reportes para cada evento registrado en cada campo de seguridad (controles de acceso, prevención de amenazas) para un mejor diagnóstico y respuesta a los incidentes.
2.4.2	La solución debe tener un mecanismo "Drill-Down" para navegación por las vistas en tiempo real sobre eventos de seguridad de alto nivel hasta los registros granulares que lo componen aplicaciones, IPS, Anti-virus, Anti-bot, filtrado URLs, usuarios, y filtro de archivos.
2.4.3	Debe tener vistas históricas (una hora, un día, una semana, un mes, o tiempo histórico personalizado).
2.4.4	La solución debe permitir la creación o personalización de vistas con filtros basados en cualquier característica del evento, como aplicación de seguridad, IP de origen y destino, servicio, tipo de evento, severidad del ataque, país de origen y destino, etc.
2.4.5	Debe soportar como tipos de eventos por lo menos: rastreos no autorizados, accesos no autorizados, anomalías de red y actividad basada en host.
2.4.6	Generar alertas automáticas vía: Email, SNMP, Syslog.
2.4.7	La solución debe permitirle al administrador agrupar eventos en función de cualquiera de sus características, incluidos varios niveles de anidación y poder exportar a PDF.
2.4.8	Debe permitir crear y personalizar reportes predefinidos, ajustando el reporte a las necesidades del administrador.
2.4.9	La solución debe soportar la programación automática de reportes para la información que se necesita de forma regular (diaria, semanal y mensual). La solución también debe permitirle al administrador definir la fecha y la hora en que el sistema de informes comienza a generar el informe programado.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

2.4.10	La solución debe admitir los siguientes formatos de informes: PDF, CSV o Excel.
2.5	CAPACIDAD DE ANÁLISIS, INVESTIGACIÓN Y RESPUESTA FRENTE A INCIDENTES DE SEGURIDAD
2.5.1	La solución debe utilizar inteligencia artificial para el rastreo de Internet buscando sitios maliciosos y evitar la conexión con ellos.
2.5.2	Utilizando capacidades de automatización, debe permitir ejecutar acciones como actualizar listas de actualización dinámica en el firewall de manera que se pueda bloquear el acceso a sitios maliciosos de forma automática.
2.5.3	La solución podrá disparar acciones y reglas automáticamente basadas en eventos o incidentes de seguridad, con capacidad de definir y aplicar reglas basadas en tipos de registro, frecuencia de los incidentes y otros criterios.
2.5.5	Todos los servicios de seguridad habilitados deben contar con capacidades de inteligencia artificial y aprendizaje de máquina en tiempo real.
2.6	MONITOREO DE MEJORES PRÁCTICAS Y CUMPLIMIENTO DE REGULACIONES
2.6.1	La consola centralizada debe incluir un módulo de monitoreo de políticas de regulaciones y mejores prácticas en la configuración de seguridad.
2.6.2	Debe incluir al menos 100 recomendaciones de mejores prácticas directas del fabricante. Adicional, recomendaciones que provienen de las regulaciones.
2.6.3	La asesoría de las regulaciones debe aplicarse en tiempo real.
2.6.4	Debe poder generar reportes automatizados para las regulaciones.
2.6.5	Las verificaciones de cumplimiento deben revisarse con cada cambio hecho en las políticas de seguridad.
2.6.6	Debe tener una sección de alertas donde se resalten violaciones a recomendaciones o regulaciones.
2.6.7	Todas las mejores prácticas deben incluir notas de recomendaciones que permita a los administradores obtener información sobre las acciones que se deben tomar para mitigar el incidente.
2.7	GARANTÍA Y SOPORTE DE FABRICANTE
2.7.1	Los equipos objeto de renovación deberán contar con soporte vigente del fabricante durante el período requerido por la Entidad.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

	La renovación deberá incluir soporte integral para los equipos y componentes objeto del proceso, incluidos el sistema operativo, los módulos de seguridad y los componentes de administración, con vigencia hasta el 21 de septiembre de 2027.
2.7.2	Durante la vigencia del licenciamiento y soporte, el fabricante deberá brindar soporte técnico, directamente o por medio de un canal autorizado con personal certificado, en modalidad 7x24 y de acuerdo con los niveles de servicio establecidos. La cobertura deberá comprender los equipos objeto de renovación, el sistema operativo, los módulos de seguridad, administración y reportes, con vigencia hasta el 21 de septiembre de 2027.
2.7.3	Deberá contemplar derecho a actualizaciones, feature packs, hot fixes y releases. acceso a soporte técnico y base de conocimiento del fabricante.
2.7.4	Deberá brindar acceso a centros de soporte técnico en línea del fabricante para asistencia técnica, soporte de resolución de problemas y escalamiento de problemas críticos, y acceso a la base de datos de conocimientos del fabricante a través de Internet.
3	ADICIONALES
3.1	El oferente deberá realizar la transferencia de conocimiento mínimo 24 horas, sobre la gestión y administración de la solución ofertada, para mínimo 3 personas que designe el SGC.
3.2	El contratista debe garantizar continuidad operativa mediante arquitectura redundante (HA) en donde aplique. Garantizar atención inmediata de fallas bajo los SLA del soporte ofrecido. Presentar compromiso de disponibilidad de equipos temporales mediante mayorista o fabricante, bajo esquema de préstamo o contingencia, sin requerir propiedad del contratista.
3.3	El Contratista debe monitorear 5* 8 de manera proactiva la solución ofertada con el fin de Alertar de los problemas mediante un correo al administrador de la solución del SGC, para permitir una solución más rápida y verificar el correcto funcionamiento de todos los servicios mediante un SOC (adjuntar un documento explicando el proceso de monitoreo y las herramientas utilizadas que garanticen este servicio).
3.4	Como parte del Servicio de Seguridad, se deberá ejecutar un análisis de vulnerabilidades que entregue un reporte detallado de los hallazgos junto con su respectivo plan de remediación.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

	Posteriormente, estos resultados deberán ser presentados y socializados ante el personal técnico de la Subdirección de Gestión de Sistemas de Información.
3.5	El oferente debe contar con la certificación ISO /IEC 27001 :2022 Y que aplique en Comercialización de soluciones de Ciberseguridad, infraestructura y servicios.

PERSONAL MÍNIMO REQUERIDO					
Item	Nombre o Cargo	Cantidad	% de Dedicación	Estudios mínimos requeridos	Experiencia mínima requerida
1	Ingeniero o Análisis Vulnerabilidades	1	100% durante fase de implementación y soporte	Profesional en ingeniería de sistemas, electrónica, telecomunicaciones y afines deberá demostrar y contar con las siguientes certificaciones: - Especialización en seguridad informática - Certificación ISO/IEC 27001:2013 - Gestión Seguridad De la Información. - Certificación ITIL - CISM (Certified Information Security Manager) vigente - Certified Ethical Hacker CEH - Endpoint Security ENS 10.7.0 - Proficiency Exam - CloudGuard WAF	Experiencia demostrada en mínimo 2 entidades en donde haya realizado, soportado análisis de vulnerabilidades.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

				Technical Specialist	
2	Ingeniero o Implementador y/o de Soporte:	1	100% durante fase de implementación y soporte	Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Telecomunicaciones o áreas afines, con tarjeta profesional vigente con certificaciones vigentes Certified Security Administrator - CCSA (vigente) Certified Security Expert CCSE (vigente)	Experiencia demostrada en mínimo dos (2) proyectos ejecutados como implementador o configurando soluciones de Firewall en alta disponibilidad.
3	Ingeniero de soporte:	1	100% durante fase de implementación y soporte	Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Telecomunicaciones o áreas afines, con tarjeta profesional vigente. certificado por el fabricante en Certified Security Expert CCSE Certified Security Master CCSM	Experiencia demostrada mínima de 3 proyectos en la configuración, instalación y soporte técnico de firewalls en alta disponibilidad

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

				Certified Troubleshooting Expert – CSTE (vigente) CloudGuard WAF – Technical Specialist vigentes	
--	--	--	--	--	--

CALIDAD DE LAS CERTIFICACIONES PARA ACREDITAR EXPERIENCIA DEL PROFESIONAL MÍNIMO REQUERIDO

Las certificaciones que acrediten la experiencia de los profesionales deben ser expedidas directamente por la empresa o entidad para la cual prestaron sus servicios. En el caso de las entidades públicas, quien certifica debe ser un servidor público jefe de la oficina de contratación correspondiente u ordenador del gasto. En el caso de las entidades privadas, quien certifica debe ser el gerente o su delegado.

El ingeniero que realizará el análisis de Vulnerabilidad debe ser un ingeniero con especialización en seguridad informática, con certificación ISO/IEC 27001:2013, CISM (Certified Information Security Manager) vigente y Certified Ethical Hacker CEH Endpoint Security ENS 10.7.0 Proficiency Exam con mínimo 2 certificaciones de experiencia en mínimo 2 entidades en donde haya realizado, análisis de vulnerabilidades. Adjuntar certificaciones.

Cada certificación y sus soportes deben permitir verificar la siguiente información:

Nombre, dirección y teléfono del empleador o contratante.

Cargo en el cual se desempeñó.

Nombre y cargo de la persona que firma la certificación.

Para la evaluación del grupo de profesionales debe adjuntarse la siguiente documentación:

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

1. Certificación vigente expedida por el Consejo Profesional correspondiente o entidad que haga sus veces que dé cuenta de la vigencia de su matrícula profesional.

Nota 1. Para los profesionales propuestos deberán aportar el certificado de antecedentes disciplinarios expedido por los respectivos Consejos Profesionales según corresponda por su profesión. Ejemplo: Consejo profesional de ingeniería COPNIA, el Consejo Profesional Nacional de Ingenierías Electrónica, Mecánica y Profesiones Afines u otros.

El contratista deberá presentar las hojas de vida del personal propuesto, junto con su respectiva documentación soporte, como parte de los entregables exigidos en el pliego de condiciones.

Nota 2. Para la verificación del PERSONAL requerido, el contratista deberá allegar fotocopias de los diplomas o actas de grado (según aplique), certificaciones, soporte de la experiencia general y específica, cédulas de ciudadanía, certificado de antecedentes disciplinarios y penales, así como de no responsable fiscal, al igual que su tarjeta profesional (según aplique)

Nota 3. El personal dependerá administrativamente del contratista y no tendrá vínculo laboral con el SGC. No obstante, éste se reserva el derecho de solicitar el retiro o reemplazo del que considere no apto o que con sus actuaciones atente contra la buena relación con el contratante, la comunidad, o cause algún impacto negativo al SGC o al ambiente laboral.

Nota 4. Para acreditar la experiencia del personal, se deben anexar certificación y/o el contrato que reúnan los siguientes requisitos:

- a) Señalar el objeto del contrato
- b) Indicar fecha de inicio y terminación del contrato
- c) Indicar el cargo ocupado dentro del contrato
- d) Indicar nombre, dirección y teléfono del contratante

Nota 5. En el evento en que las certificaciones no contengan toda la información solicitada, el contratista debe anexar el contrato o el acta de liquidación de éste, de tal forma que la información no contenida en la certificación se complementa con el contenido de dichos documentos. Además de los contratos y las certificaciones o demás documentos que acreditan la experiencia del personal, el contratista deberá adjuntar los siguientes documentos:

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

a) Copia de la tarjeta o matrícula profesional vigente, junto con los antecedentes disciplinarios profesionales.

b) Copia del acta de grado o diploma de título profesional y de especialización, si a ello hubiere lugar.

Nota 6: Los anteriores requerimientos son de obligatorio cumplimiento y deberán tenerse en cuenta al momento de que el proponente elabore su oferta económica.

Nota 7: Todos los requisitos mencionados anteriormente se entienden que son cumplidos y aceptados por el proponente con la suscripción del presente anexo.

Nota 8: En caso de que el proponente no presente el anexo técnico o este se presente sin la firma del representante legal, la propuesta será rechazada. Lo anterior teniendo en cuenta que lo plasmado en dicho anexo son requerimientos técnicos mínimos de obligatorio cumplimiento.

EXPERIENCIA DEL PROPONENTE

El proponente debe acreditar la experiencia específica mínima habilitante aportando máximo tres (3) CONTRATOS terminados o liquidados, celebrados con entidades públicas o privadas en el o los cuales acredite la experiencia solicitada en el presente numeral.

La experiencia certificada deberá estar inscrita en el registro único de proponentes RUP, y cumplir por lo menos dos (2) de los códigos del Clasificador de Bienes y Servicios establecidos para el presente proceso.

Segmento		Familia		Clase	
Código	Nombre	Código	Nombre	Código	Nombre

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

43	Difusión de Tecnologías de Información y Telecomunicaciones	23	Software de computador	32	Software de seguridad y protección
43	Difusión de Tecnologías de Información y Telecomunicaciones	23	Software de computador	29	Software de redes
43	Difusión de Tecnologías de Información y Telecomunicaciones	22	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	26	Equipo de servicio de red
43	Difusión de Tecnologías de Información y Telecomunicaciones	22	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	25	Equipo de seguridad de red
81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios de informática	18	Servicios de sistemas y administración de componentes de sistemas
81	Servicios Basados en Ingeniería, Investigación y Tecnología	11	Servicios de informática	15	Ingeniería de software o hardware
43	Difusión de Tecnologías de Información y Telecomunicaciones	23	Software de computador	26	Software específico para la industria

NOTA 1: Igualmente se determina como parte de la experiencia habilitante del proponente las siguientes características o alcances, para

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

lo cual el proponente debe aportar las respectivas certificaciones y/o documentación de los contratos presentados que permita su validación:

- Contratos suscritos y ejecutados, cuyo alcance incluya actividades de venta, adquisición, o renovación de soluciones de seguridad perimetral y Firewall en Alta disponibilidad del mismo fabricante que actualmente tiene el SGC. Como mínimo uno (1) de los contratos acreditados debe incluir la solución SDwan incluido en cada uno de los modelos de Firewall solicitados
- La experiencia debe estar relacionada con el objeto de esta convocatoria pública, el alcance debe incluir actividades de venta, adquisición, o renovación de soluciones de seguridad perimetral, Firewall en Alta Disponibilidad.

El proponente debe ser distribuidor autorizado del fabricante de los equipos a renovar, lo cual debe acreditar, mediante presentación de certificación vigente, expedida por el representante en Colombia, no mayor a 15 días anteriores a la fecha del cierre de la presente Convocatoria Pública y dirigida Al SERVICIO GEOLOGICO COLOMBIANO, donde se especifique que se encuentra autorizado para licenciar, vender y soportar técnicamente las soluciones de seguridad en Colombia. La certificación debe indicar que el proponente cuenta con certificación CCSP (Certified Collaborative Support Provider), que tiene nivel mínimo de Premier Partner o superior.

El proponente deberá entregar la documentación técnica detallada de toda la actualización realizada

El proponente deberá entregar un informe técnico mensual durante el tiempo de garantía y/o soporte sobre el desempeño de la plataforma mantenida

Deberá realizar análisis previo de la plataforma tecnológica actual: hardware, software, red de comunicaciones, condiciones ambientales y sistemas de información.

Deberá efectuar Transferencia de conocimientos en los productos ofrecidos.

El proponente debe brindar capacitación y transmisión de conocimientos de la renovación sobre la solución instalada.

	FORMATO	CÓDIGO	F-CIN-EPS-003
	SOLICITUD DE INFORMACIÓN PROVEEDORES	VERSIÓN	1
		CLASIFICACIÓN DE LA INFORMACIÓN	PÚBLICA

Realizar las pruebas necesarias para garantizar el buen funcionamiento de la solución.

Efectuar Administración, Seguimiento, monitoreo a los equipos objeto del contrato.

Para la prestación del servicio se requiere que el proponente cuente con un esquema de mesa de ayuda, donde se puedan generar los reportes de incidentes frente a la prestación del servicio. Adjuntar Metodología y mencionar el software con el cual realiza esta función.

Detectar y reaccionar oportunamente ante incidentes de seguridad de la información, de acuerdo con los niveles de servicio (SLAs).

Brindar constantemente recomendaciones que permitan obtener un mejor nivel de mitigación de riesgos derivados del uso de la tecnología.

Se debe brindar un componente de alarma para la detección automática de eventos de seguridad, que faciliten la gestión de estos sobre la infraestructura tecnológica

En caso de no ser posible la solución remota o telefónica, se requiere prestación del servicio en sitio, de acuerdo con los niveles de servicio pactados

Se requiere servicio de análisis de log y generación de reportes de manera periódica.

El contratista deberá brindar soporte remoto y/o en sitio dependiendo el nivel de criticidad de la solicitud realizada para fallas e implementaciones.

Dentro del Servicio de Seguridad debe realizar un análisis de vulnerabilidades que incluya lista de Vulnerabilidades encontradas con su respectivo plan de remediación, efectuando la presentación y socialización al personal técnico de la Subdirección de Gestión de Sistemas de Información.