ANEXO TECNICO No.1
SEGURIDAD PERIMETRAL

OBJETO: Renovación del licenciamiento de la solución de seguridad Perimetral – FORTINET de la Agencia ITRC

ITEM	1. DESCRIPCION SOLUCION DE SEGURIDAD RED PERIMETRAL	CANT	Cumple (SI /NO)
1	Renovación y/o actualización FW FortiGate 400E con S/N: FG4H0ETB20904786 (Primary) FG4H0ETB20904699 (Secondary) 12 meses a partir del vencimiento del licenciamiento actual	2	
2	Renovación y/o actualización FAZ150G Serial FAZ15GT221000032 IOC+OUTBREAK DETECTION 12 meses a partir del vencimiento del licenciamiento actual	1	
ITEM	**Requerimientos Generales**		**Cumple (SI /NO)**
1	Las renovaciones son requeridas por el periodo de un año en un esquema 7 x 24 ante fabricante y con las siguientes características de las plataformas para los seriales mencionados, las cuales se describen a continuación:		
2	Derecho a actualización de Firmware		
3	Acceso al portal de soporte y recursos técnicos asociados.		
4	Elaboración de informes sobre incidentes técnicos (mediante la web, chat o teléfono)		
5	El servicio de soporte incluido en el licenciamiento debe contemplar la atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas, etc.		
6	El oferente debe incluir todo el Software necesario para dar cumplimiento a lo requerido en el presente proceso.		
ITEM	**Especificaciones de Renovación y/o Actualización FORTIGATE**		**Cumple (SI /NO)**
7	La renovación y/o actualización entregada por el oferente debe contemplar mínimo los siguientes requerimientos:		
8	Módulo de detección y prevención de intrusos (IPS) para encontrar patrones basados en ataques y realizar las acciones oportunas para bloquear dichos ataques. El Desempeño esperado después de la actualización debe ser mínimo de 7 Gbps.		
9	Modulo antivirus inteligente que pueda ser ajustado a diferentes tipos de políticas por aplicaciones o tráfico, permitir tomar acciones preventivas antes de entrar o salir de la plataforma. El Desempeño esperado después de la actualización debe ser mínimo de 5 Gbps para Threat Protection.		
10	Modulo para Bloqueo de contenido Web basado en listas blancas/negras de URL y palabras clave, filtrado de páginas Web basado en categorías (77) y/o clasificaciones, utilizando el Servicio de Fortiguard Web Filtering, con cobertura 24×7 a nivel mundial, que proviene de más de 50 servidores de distribución instalados en 12 diferentes localidades alrededor del mundo, cuotas de uso basadas en tiempo, por categoría: permite otorgar y administrar el uso de recursos de una manera responsable, limitando así posibles abusos. Clasificación de imágenes contenidas en URL.		
11	Módulo de aplicación de políticas basadas en diferentes tipos de conexión (Interfaces de conexión física o virtual) o por métodos de autenticación de usuario (Directorio activo o usuario local).		
12	Debe estar habilitada la interconexión para protocolos de red IPv4 e IPv6. Asi mismo se requiere contar con conectividad a mínimo 1Gbps con interfaces RJ-45 y SFP.		
13	Modulo para configurar anchos de banda en las políticas y SD-WAN.		

14	Modulo para habilitar o bloquear aplicaciones basadas en bases de datos actualizadas constantemente.	
15	Se debe contar con un módulo de inspección SSL/SSH para encontrar posibles amenazas bajo sistema de encriptación tanto en archivos descargados como correos electrónicos. El Desempeño esperado después de la actualización debe ser mínimo de 4.8 Gbps para SSL Inspection.	
16	Módulo de configuración de VPN (Site to Site y Client to Site) para conexiones seguras externas que permitan dar un alto nivel de seguridad y cifrado entre la red del Senado y conexiones externas.	
17	Debe incluir módulo de Security Rating con la finalidad de auditar la configuración en tiempo real de la plataforma e indicar las mejores prácticas y sugerencias sobre la misma.	
ITEM	**2.SERVICIOS PROFESIONALES Y DE SOPORTE INCLUIDOS EN LA RENOVACION**	**Cumple (SI /NO)**
1	El oferente deberá entregar todas las licencias en los sitios/sedes indicadas por la entidad.	
2	El oferente deberá realizar la implementación en los sitios/sedes indicadas por la entidad.	
3	El oferente deberá realizar la renovación de los equipos con personal certificado.	
4	El oferente deberá contar con la certificación ISO 27001 e ISO 9001 en sus procesos, ya que este proceso al ser una implementación de plataformas de seguridad informática, demanda que el contratista cuente con ella, la cual ratifica su idoneidad y la de la implementación a realizar.	
5	El oferente deberá adjuntar con su propuesta una carta emitida por el fabricante donde evidencie el nivel de membresía más alto en las plataformas ofertadas y la prestación de un servicio idóneo y profesional de la plataforma con la que cuenta la entidad.	
6	El oferente deberá contar con una certificación o documento oficial del fabricante en donde demuestre que está catalogado como partner de servicios preferido y que cuenta con la habilidad de prestar servicios sobre sus soluciones de seguridad.	
8	Dentro de los servicios incluidos en el licenciamiento se debe tener en cuenta la actualización de las licencias de las soluciones con las que cuenta la entidad, así como su entrega a satisfacción, realizando todas las actividades necesarias para cumplir con el objeto, sin que esto genere gastos o cobros adicionales para la entidad.	
9	Se deben considerar como mínimo los siguientes parámetros para la renovación y/o actualización de los Firewalls: - Levantamiento de información para la configuración. - Actualizaciones disponibles durante la vigencia.	
ITEM	**EQUIPO DE TRABAJO MINIMO**	**Cumple (SI /NO)**
11	El personal propuesto deberá realizar el soporte, configuraciones, mantenimiento, actualizaciones y puesta en marcha de las mismas sobre la solución ofertada (si se requiere), y para garantizar su experiencia en los productos ofertados deberán estar certificados por el fabricante en mínimo a nivel especialista y, al menos uno, deberá contar con los niveles de asociado, profesional y especialista emitidos por la marca (deberá adjuntar la escala de certificación del fabricante o link público para encontrar la mismas, con el fin de tener claridad de los respectivos niveles de certificación).	

12	Adjuntar certificados vigentes del fabricante, con el fin de garantizar que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante. Adicionalmente al menos uno de los perfiles deberá estar certificado como CEH (Certified Ethical Hacker).	
ITEM	**SERVICIOS DE SOPORTE INCLUIDOS EN LA RENOVACION**	**Cumple (SI /NO)**
14	El contratista deberá proveer soporte para la solución mencionada en un esquema 7x24, por 12 meses para los equipos Fortigate.	
15	Manejo de atención a incidentes operativos, interrupciones no planificadas del servicio, o reducción en la calidad del mismo.	
16	Consultas a través de llamadas telefónicas, correo electrónico y contar con una plataforma de tickets donde se pueda llevar registros de los casos.	
17	Sesiones remotas y atención en sitio (En caso de requerirse). Todo con respecto a las plataformas ofertadas y objeto del presente contrato.	
18	Para las solución Fortigate se requieren mínimo 2 visitas de mantenimiento que incluyen revisión de configuración, desempeño y recomendaciones. (En caso de requerirse)	
20	El oferente debe contar con un SOC (Security operation center) con el fin de brindar el servicio de soporte el cual debe incluir atención de incidentes sobre la plataforma ofertada. Este deberá estar certificado en ISO 27001 e ISO 9001 y pertenecer al grupo de respuesta a incidentes FIRST, LACNIC-CSIRT para evidenciar y acreditar su experiencia como SOC.	
21	El proponente deberá acreditar experiencia como mínimo en los productos del código de clasificación iniciado con “43” y dos (2) servicios con código de clasificación que inicie con “81”, indicados en los estudios previos.	
ITEM	**CERTIFICACIONES DE FABRICANTE**	**Cumple (SI /NO)**
22	Se debe entregar junto con la propuesta certificación emitida directamente de los fabricantes de las soluciones ofertadas donde se evidencie que son distribuidores autorizados y se encuentran en la categoría más alta del programa de canales del fabricante.	
ITEM	**TRANSFERENCIA DE CONOCIMIENTO INCLUIDO EN LA RENOVACION**	**Cumple (SI /NO)**
23	El fabricante y/o proveedor debe contar dentro de su esquema de transferencia de conocimiento, un portal de capacitaciones sin costo adicional, donde se encuentre sesiones técnicas sobre la solución ofertada. Estás capacitaciones deben ser en español, las personas de la entidad deben poder inscribirse a estos cursos y tomarlos en vivo y en directo con un capacitador del fabricante, el fabricante debe tener disponibilidad de estos cursos al menos 1 vez al mes dentro del portal.	

Con la firma del presente anexo técnico, manifiesto que entendemos y cumplimos todos los requerimientos establecidos para satisfacer la necesidad de la agencia ITRC.

Firma:
Nombre: *Representante Legal*
Cédula: