Código de la dependencia productora

Bogotá D.C.,

NOMBRE DEL DESTINATARIO
Cargo
Nombre de la entidad
Teléfono:
Correo Electrónico:
Ciudad y departamento
País

Asunto: SOLICITUD DE INFORMACIÓN PARA ESTUDIO DE MERCADO

Respetados señores:

Atentamente solicito su colaboración, a efectos de obtener información para consolidar estudios de mercado sobre los bienes, obras y/o servicios que se citan a continuación:

OBJETO	Adquirir la actualización tecnológica de las consolas de Firewall para el MHCP	
UNSPSC	**CÓDIGO UNSPSC**	**DESCRIPCIÓN**
	81111800	Servicios de sistemas y administración de componentes de sistemas
	81112200	Mantenimiento y soporte de software
	81112300	Mantenimiento y soporte de hardware de computador
	43222500	Equipo de seguridad de red
	43233200	Software de seguridad y protección
	81112500	Servicios de alquiler o arrendamiento de licencias de software de computador
	Nota: Por favor indicar el código en el cual está clasificado el bien o servicio a contratar.	
DESCRIPCIÓN Y/O ALCANCE	**ESPECIFICACIONES TÉCNICAS MÍNIMAS**	**COTIZACIÓN ALTERNATIVA**
	Ver anexo **No. 1**	En caso de que aplique o se requieran
DURACION DEL CONTRATO	El término de duración del contrato que se suscriba será hasta el 30 de noviembre del 2024, inclusive, contados a partir de la expedición del correspondiente registro presupuestal y aprobación de las garantías que debe constituir el contratista.	

PLAZO PARA LA ENTREGA DE LOS BIENES Y/O SERVICIOS	El plazo para la entrega de bienes será hasta el 30 de septiembre del 2024 inclusive.
LUGAR DE EJECUCIÓN	La ejecución del contrato será la ciudad de Bogotá, D.C. en las instalaciones del Ministerio de Hacienda y Crédito Público y de manera virtual en el evento de requerirse, previa autorización del Supervisor del contrato, bajo herramientas tecnológicas autorizadas por el Ministerio de Hacienda y Crédito Público en la ciudad de Bogotá.
FORMA DE PAGO	EL MINISTERIO pagará al CONTRATISTA, una vez se encuentre aprobado el P.A.C. (Programa anual mensualizado de caja), el valor del contrato de la siguiente forma:

VIGENCIA	DESCRIPCION	PRODUCTO O ACTIVIDAD
2024	Un pago del presupuesto correspondiente al del valor de la adquisición de las consolas de firewall con el fabricante Check Point, relacionadas en el numeral 1, incluidos Soporte y Garantía del Anexo “REQUERIMIENTOS TECNICOS MINIMOS”, resultante del evento de subasta	Documento con la relación de la entrega de las consolas de firewall y soporte con el fabricante.
	Un pago del presupuesto correspondiente al valor de la instalacion e implementacion de las consolas de firewall (ítems 1 y 2), resultante del evento de subasta	Documento de la implementación realizadas para las consolas de firewall.

Dichos pagos se efectuarán con sujeción a la disponibilidad de PAC, dentro de los diez (10) días hábiles siguientes a la radicación en SECOP y la debida suscripción del acta de recibo a satisfacción, recibo de elementos por el grupo de almacén del Ministerio, presentación de la factura y del cumplido expedido por el supervisor designado y la certificación de pago de aportes parafiscales y de seguridad social por parte del contratista.

VALIDEZ DE LA COTIZACIÓN	

COTIZACIÓN ALTERNATIVA *	
Detallar: CUANDO COMPRENDA VARIOS ÍTEMS, SE DEBE COTIZAR INDIVIDUALMENTE CADA UNO	**VALOR UNITARIO**

VALOR TOTAL (incluido IVA)	

NOTA: Si el cotizante encuentra que algo falta, no es procedente o es diferente a lo consignado en la descripción técnica de la necesidad, es importante que lo manifieste, justificando la razón que sustenta el cambio, para que el ministerio, previo análisis, determine la procedencia de la sugerencia. Para tal fin deberá determinar los costos de la cotización alternativa.

Agradecemos se sirva remitir la información respectiva a más tardar el día 15 de marzo de 2024, a través de correo electrónico invtecnologia@minhacienda.gov.co o german.castro@minhacienda.gov.co o a la siguiente dirección: Carrera 8 No. 6C-38 de la ciudad de Bogotá a nombre de la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público**.**

Cordialmente,

RICARDO FERNELIX RIOS ROSALES
Director de Tecnología

Anexos:

* Si el cotizante desea presentar una cotización alternativa a la solicitada por el Ministerio, debe cumplir con las condiciones técnicas mínimas de la cotización básica.

ANEXO No.1
REQUERIMIENTOS TÉCNICOS

1.	**REQUERIMIENTOS GENERALES** La actualización tecnológica de las consolas de Firewall para el MHCP se refiere al cambio de las consolas actuales que se encuentran por fuera de soporte del fabricante por nuevas consolas, las cuales deben ser entregadas, instaladas y configuradas como una solución integrada a la infraestructura de seguridad perimetral que actualmente tiene en uso el Ministerio con las siguientes características:
1.1.	Proveer las consolas para la gestión de la infraestructura de seguridad perimetral relacionada en el presente numeral, con entrega o, instalación, implementación y migración de acuerdo con la siguiente descripción: **Ítem** / **Descripción** 1 — Consolas para la gestión de políticas de las soluciones de firewalls perimetrales de SIIF Nación. 2 — Consolas para la gestión de políticas de las soluciones de firewalls perimetrales del Ministerio de Hacienda y Crédito Público **NOTA**: La solución hace referencia al hardware, software, herramientas de administración, licencias y demás componentes que se requiera para su correcto funcionamiento de conformidad con los requerimientos técnicos mínimos contenidos en el presente anexo.
1.2.	Las actividades que resulten para la actualización de las soluciones descritas en el numeral 1.1, se deben realizar bajo las siguientes condiciones: **a)** Acompañamiento permanente por parte de expertos del fabricante Check Point previas a la implementación , migración y estabilización. **b)** Soporte permanente en línea con el fabricante Check Point de tal forma que los eventos que se presenten sean atendidos y corregidos de forma oportuna, sin que se genere interrupción de los servicios. El servicio de soporte debe ser prestado por el tiempo de garantía requerido, es decir por tres (3) años. **c)** Entregar documentación del plan de ejecución, de la infraestructura y de las actividades de , implementación, migración y estabilización realizadas. Hacer entrega de ésta a la supervisión del contrato. **d)** Las consolas de gestión deberán quedar debidamente migradas, instaladas, configuradas, puestas en producción y licenciadas con todas las funcionalidades solicitadas en el presente anexo.

	e) Tanto el hardware como el software de las consolas instaladas deberán tener la versión recomendada por el fabricante Check Point y que se integre con la versión del software instalada en las soluciones de firewall de las infraestructuras de SIIF Nación y MHCP. **f)** Ofrecer las consolas de gestión de políticas en alta disponibilidad, para lo cual deben entregar, actualizar, licenciar, configurar e integrar los componentes o software adicional que se requieran y sus costos deben ser incluidos en la misma.
1.3.	El contratista deberá contemplar todos los elementos y los recursos necesarios para la instalación, implementación, migración, integración y funcionamiento de las consolas con las soluciones de firewall de las infraestructuras de MHCP y SIIF NACIÓN, a fin de garantizar el perfecto funcionamiento y operatividad sin generar costos adicionales para la Entidad.
1.4.	Con el fin de integrar las consolas de gestión de políticas adquiridas, el contratista deberá validar la plataforma actual de las soluciones de seguridad perimetrales de las infraestructuras de MHCP y SIIF NACIÓN, para lo cual se requiere: **a)** Con el fin de plantear las actividades para la migración e implementación, el contratista debe validar los servicios, tráfico y configuraciones que actualmente se encuentran implementados **b)** Presentar un diagrama de la infraestructura al Ministerio en el que incluya las consolas solicitadas en conjunto con las soluciones de firewalls actuales de la infraestructura del MHCP y SIIF NACIÓN. Dicho diagrama se debe presentar al supervisor del contrato dentro de los primeros 15 días hábiles posteriores al inicio de la ejecución del contrato. **c)** Elaborar el plan de trabajo basado en el análisis realizado, las recomendaciones del fabricante, las mejores prácticas del mercado y las opciones de mejora, para la instalación, configuración, migración de las consolas de gestión descritas en el numeral 1.1. y la integración con las soluciones de firewalls actuales. Dicho plan de trabajo se debe presentar al supervisor del contrato dentro de los primeros 20 días hábiles posteriores al inicio de la ejecución del contrato. **d)** Ejecutar las labores definidas en el plan de trabajo a fin de garantizar la correcta instalación, configuración, implementación, migración, optimización e integración de las consolas de gestión, con las funcionalidades y servicios requeridos y aplicando las políticas, normas y procedimientos fijados por el Ministerio. La ejecución de estas labores deberá realizarse bajo la modalidad de control de cambio en ventanas de tiempo acordadas con la supervisión del contrato, de tal forma que no se presente afectación de los servicios que tiene la Entidad.
1.5.	Realizar las pruebas pertinentes con el fin de garantizar el correcto funcionamiento de las soluciones. Como mínimo se deberá realizar las siguientes pruebas: **a)** Conectividad **b)** Alta disponibilidad **c)** Integración con las soluciones de firewall respectivas **d)** Funcionalidades solicitadas Las pruebas efectuadas se realizarán en horario que no interrumpan los servicios que actualmente se encuentran en operación en la Entidad. Las pruebas y la hora en la cual se efectúen serán

	avaladas por el Ministerio y se programarán de forma independiente para los ítems 1 y 2 del numeral 1.1 del presente anexo.
1.6.	El contratista debe proveer todos los elementos necesarios para la instalación de los equipos en racks estándar de 19 pulgadas (rieles, conectores, cables de poder, entre otros). Los racks son suministrados por el Ministerio.
2.	Prestar durante tres años a partir de la firma del acta de entrega de bienes y servicios a satisfacción para el ítem 2 y posterior al 1ro de octubre de 2024 para el ítem 1, el servicio de asistencia técnica con el fabricante Check Point "Enterprise Software Subscription and Premium Support (7 x 24)" o como se denomine en el momento de inicio del contrato, incluyendo como mínimo los siguientes servicios: a) Actualizaciones de software, parches y services packs liberados. b) Acceso a las bases de datos de conocimiento de soporte y foros de los productos. c) Abrir o escalar casos directamente al fabricante para casos de criticidad e impacto alto y recibir soporte remoto o telefónico 30 minutos después de abierto el caso. d) Reemplazo de los equipos por fallas definitivas.
3.	**ITEM 1: CONSOLAS PARA LA GESTIÓN DE POLÍTICAS DE LAS SOLUCIONES DE FIREWALLS PERIMETRALES DE SIIF NACIÓN.**
CARACTERISTICAS TECNICAS GENERALES DE LA SOLUCIÓN	
3.1.	Las consolas de gestión deben tener las siguientes características: **a)** Solución de propósito específico para seguridad, conformada por equipos físicos denominados "*Appliance*". **b)** Licenciamiento del software requerido para la solución adquirida con su correspondiente garantía y soporte técnico cubiertos por el fabricante. El servicio de soporte debe ser prestado por tres (3) años (Ver numeral 2) **c)** Equipos implementados en alta disponibilidad, de manera tal que, ante la falla de uno de los equipos, otro pueda asumir los servicios y la carga de forma automática del equipo que falla, sin restricción de tiempo, de servicio, ni recurso con relación al funcionamiento normal en producción, garantizando la continuidad de los niveles de seguridad y servicios implementados de forma transparente a los usuarios. **d)** Las consolas de gestión deben ser instaladas en los dos (2) Datacenter de la Entidad y garantizar la alta disponibilidad en cada Datacenter. El Ministerio proporcionará VLAN Extendida y/o enrutamiento entre Datacenters. **e)** La conmutación en caso de falla de alguno de los appliances no debe implicar la perdida de conexiones (es decir no deben reestablecerse nuevas sesiones, en caso de falla de alguno de los nodos). **f)** Las consolas de gestión centralizada y unificada deben gestionar y visualizar de manera integral las funcionalidades de las actuales soluciones de firewall perimetral de SIIF NACION. A este sistema se deben migrar las funcionalidades, políticas y configuraciones que actualmente la Entidad tiene implementadas y realizar las mejoras a que haya lugar.

	g) Cada una de las consolas deberán tener la capacidad de almacenar mínimo de 4TB (RAID-1) de registros de información y que estos registros se puedan acceder de manera inmediata en caso de requerir una consulta en el tiempo.
3.2.	Se debe realizar la migración de las configuraciones y funcionalidades que se tienen implementadas en las actuales consolas de gestión: **a)** Políticas de acceso de Firewall **b)** Políticas de traslación **c)** Control de Aplicaciones **d)** Intrusion Prevention System **e)** Control de Malware Conocido (Antivirus/Antimalware) **f)** Control de Bots **g)** Control de Datos **h)** Módulo de Adquisición de Identidades **i)** Módulo VPN IPSec **j)** Módulo VPN SSL **k)** Geolocalización Así como las nuevas funcionalidades de protección incluidas en el software de las consolas de gestión adquiridas.
3.3.	Las consolas de gestión de políticas deben contar con las siguientes características: **a)** Permitir que las comunicaciones entre todos los componentes que pertenezcan a la solución total (gestión y administración, reportes, equipos de la solución de seguridad perimetral), establezcan comunicaciones seguras. **b)** Los dos equipos appliances se deben configurar en alta disponibilidad y mantenerse sincronizados automáticamente, permitiendo la administración compartida de cada firewall físico o virtual. **c)** Cada consola debe incluir las siguientes características de la serie Smart-1 600-M Plus Security Management: **a.** 4TB Raid 1de almacenamiento **b.** 64 GB RAM **c.** 4 puertos cobre GbE **d.** 1 puerto de consola **d)** Contar con la capacidad de gestionar al menos 50 dispositivos virtuales o físico. **e)** Funcionar en un esquema de alta disponibilidad, para evitar que exista pérdida de funcionalidad de administración. **f)** Realizar sobre las consolas de gestión adquiridas la integración con la solución de firewall perimetral del SIIF NACIÓN. **g)** Realizar la migración y actualización de las configuraciones y políticas de los sistemas de administración con que cuenta la Entidad.

	h) Realizar la integración con la solución de consolidación de reportes y eventos con que cuenta la solución actual de firewalls perimetrales de SIIF NACION. **i)** Incluir una herramienta de búsqueda, que permita fácilmente filtrar objetos de red, servicios, nombre de usuarios, redes, entre otros. Debe también incluir la opción de buscar objetos duplicados (con la misma IP), objetos no usados (en una regla o política) y una lista de las reglas en que un objeto especifico es usado. **j)** Tener la capacidad de hacer auditorias de las acciones de cada administrador que acceda a la plataforma. **k)** Permitir realizar un completa auditoria, seguimiento en los cambios y evolución de las políticas de seguridad. **l)** Contar con un mecanismo de revisión de políticas, previo a la instalación de las mismas, que ayude a buscar y corregir errores. **m)** La solución debe tener la capacidad de asignar politicas de acceso basadas en url, nombres de usuario, aplicaciones, dominios y no solamente por dirección ip. **n)** Incluir un contador de acceso para cada regla de seguridad o generar un reporte que presente la utilización de cada una de las reglas. **o)** Los componentes de la solución deben ser accesibles a través de SSH o de interfaz Web usando SSL **p)** La plataforma debe ser capaz de construir políticas sin importar si estas referencian a objetos o servicios IPv4 o IPv6. **q)** Tener la capacidad de forma nativa en tiempo real, de dar información sobre el estado de los dispositivos administrados (conectividad, nivel cpu, tráfico de red) e ilustrar de forma gráfica al menos eventos como la conexión de usuarios remotos vía VPN, estado de los túneles IPSEC y tráfico más común sobre las interfaces (monitor), IPS, ANTIBOT, mayores intentos de conexiones entrantes y salientes. **r)** Configurar restricciones por direcciones IP (direcciones individuales, rangos, nombres de equipos) que pueden tener control sobre la consola de administración central. **s)** Debe tener la posibilidad de definir expiración de reglas de forma automática, por fecha y hora. **t)** Configurar restricciones por geolocalización. **u)** La autenticación de administradores a las consolas de gestión de políticas debe configurarse por lo menos con alguno de los siguientes mecanismos: contraseña o certificados digitales propios de la solución de seguridad o sistemas RADIUS. **v)** Configurar roles de administración. **w)** Permitir la creación de filtros en los logs basados en cualquiera de las características del evento, tales como: firewall virtual o físico, IP de origen y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, país de origen o destino, entre otros. **x)** Presentar la distribución de eventos por países.

	y) Permitir agrupar los eventos con base en cualquier característica de estos, pudiendo agrupar en varios niveles. **z)** Permitir realizar búsquedas dentro del listado de eventos. **aa)** Incluir reportes predefinidos con los eventos detectados en la última hora, día, semana y mes. Incluyendo al menos Eventos top, Orígenes top, Destinos top, Servicios top, Orígenes top con sus eventos top, Destinos top con sus eventos top y Servicios top con sus eventos top y estado de las VPN. **bb)** Permitir la programación de reportes para que se ejecuten automáticamente para extraer información en periodos regulares de tiempo (diarios, semanales y mensuales). También debe permitir al administrador ver la fecha y horario en que empezará a generar el reporte agendado. **cc)** Soportar los siguientes formatos de reportes: HTML, CSV **dd)** Permitir la distribución automática de los reportes por correo electrónico, subiéndolos en un servidor FTP/Web y utilizando un script externo para la distribución del reporte. **ee)** Proveer reportes de información consolidada sobre al menos: **i.** Top de eventos por origen **ii.** Top de eventos por destino **iii.** Eventos por fecha. **iv.** Eventos por semana. **v.** Top de eventos por producto **vi.** Top de eventos por servicios. **vii.** Severidad **viii.** Producto **ix.** Geolocalización **ff)** Los reportes deben poder generarse en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real. **gg)** Debe soportar la integración con Active Directory mínimo con Microsoft 2012 R2 y Microsoft 2016 independiente sí es IPv4 o IPv6 **hh)** La solución debe ser capaz de adquirir la identidad de los usuarios, desde un Directorio Activo Microsoft 2012 R2 y Microsoft 2016 sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft. **ii)** La solución debe permitir la generación de backup y restauración de las configuraciones, políticas y logs permitiendo al administrador programar la realización de los backups en el tiempo deseado. **jj)** Los backups deben poderse almacenar localmente y transferir automáticamente vía FTP o SCP a un equipo que defina el Ministerio.

4.	**ITEM 2 CONSOLAS PARA LA GESTIÓN DE POLÍTICAS DE LAS SOLUCIONES DE FIREWALLS PERIMETRALES DEL MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO.**
CARACTERISTICAS TECNICAS GENERALES DE LA SOLUCIÓN	
4.1.	Las consolas de gestión deben tener las siguientes características: a) Solución de propósito específico para seguridad, conformada por equipos físicos denominados "*Appliance"*. b) Licenciamiento del software requerido para la solución adquirida con su correspondiente garantía y soporte técnico cubiertos por el fabricante. El servicio de soporte debe ser prestado por tres años (ver numeral 2). c) Equipos implementados en alta disponibilidad, de manera tal que, ante la falla de uno de los equipos, otro pueda asumir los servicios y la carga de forma automática del equipo que falla, sin restricción de tiempo, de servicio, ni recurso con relación al funcionamiento normal en producción, garantizando la continuidad de los niveles de seguridad y servicios implementados de forma transparente a los usuarios. d) Las consolas de gestión deben ser instaladas en los dos (2) Datacenter de la Entidad y garantizar la alta disponibilidad en cada Datacenter. El Ministerio proporcionará VLAN Extendida y/o enrutamiento entre Datacenters. e) La conmutación en caso de falla de alguno de los appliances no debe implicar la perdida de conexiones (es decir no deben reestablecerse nuevas sesiones, en caso de falla de alguno de los nodos) f) Las consolas de gestión centralizada y unificada deben gestionar y visualizar de manera integral las funcionalidades de las actuales soluciones de firewall perimetral de la infraestructura de Ministerio. A este sistema se deben migrar las funcionalidades, políticas y configuraciones que actualmente la Entidad tiene implementadas y realizar las mejoras a que haya lugar. g) Cada una de las consolas deberán tener la capacidad de almacenar mínimo de 6x4TB HDD de registros de información y que estos registros se puedan acceder de manera inmediata en caso de requerir una consulta en el tiempo, en las mismas consolas ofertadas. h) Proveer el servicio de reporteador en la consola de gestión de políticas que se configure como primaria.
4.2.	Se debe realizar la migración de las configuraciones y funcionalidades que se tienen implementadas en las actuales consolas de gestión: **a)** Políticas de acceso de Firewall **b)** Políticas de traslación

	c) Control de Aplicaciones **d)** Intrusion Prevention System **e)** Control de Malware Conocido (Antivirus/Antimalware) **f)** Control de Bots **g)** Control de Datos **h)** Módulo de Adquisición de Identidades **i)** Módulo VPN IPSec **j)** Módulo VPN SSL **k)** Políticas de Threat Prevention **l)** Geolocalización Así como las nuevas funcionalidades de protección incluidas en el software de las consolas de gestión adquiridas.
4.3.	**FUNCIONALIDAD SOLUCIÓN CUMPLIMIENTO NORMATIVO Y REGULATORIO** **a)** Proveer una solución que mida el nivel de cumplimiento de la configuración y parametrización de los firewalls perimetrales de MHCP, de tal forma que estos tengan la capacidad de validar las configuraciones que se realicen en ellos frente a normativas, regulaciones, estándares y mejores prácticas de seguridad informática, como ISO 27000 y NIST. **b)** La funcionalidad debe identificar riesgos de seguridad en la parametrización de los firewalls, frente a normativas, regulaciones, estándares y mejores prácticas enfocadas a la seguridad informática. **c)** Proveer y generar informes de auditoría alineados a ISO 27000, NIST, entre otros.
4.4.	Las consolas de gestión de políticas deben contar con las siguientes características: **a)** Permitir que las comunicaciones entre todos los componentes que pertenezcan a la solución total (gestión y administración, equipos de la solución de seguridad perimetral), establezcan comunicaciones seguras. **b)** Los dos equipos appliances se deben configurar en alta disponibilidad y mantenerse sincronizados automáticamente, permitiendo la administración compartida de cada firewall físico o virtual. **c)** Cada consola debe incluir las siguientes características de la serie Smart-1 6000-L Base Gen-6 Security Management (CPAP-NGSM6000L-BASE): a. 6x4TB HDD almacenamiento b. 96 GB RAM c. 4 puertos cobre GbE d. 1 puerto de consola **d)** Funcionar en un esquema de alta disponibilidad, para evitar que exista pérdida de funcionalidad de administración. **e)** Realizar sobre las consolas de gestión adquiridas la integración con la solución de firewall

	perimetral del MHCP. **f)** Realizar la migración y actualización de las configuraciones y políticas de los sistemas de administración con que cuenta la Entidad. **g)** Incluir una herramienta de búsqueda, que permita fácilmente filtrar objetos de red, servicios, nombre de usuarios, redes, entre otros. Debe también incluir la opción de buscar objetos duplicados (con la misma IP), objetos no usados (en una regla o política) y una lista de las reglas en que un objeto especifico es usado. **h)** Tener la capacidad de hacer auditorias de las acciones de cada administrador que acceda a la plataforma. **i)** Permitir realizar un completa auditoria, seguimiento en los cambios y evolución de las políticas de seguridad. **j)** Contar con un mecanismo de revisión de políticas, previo a la instalación de las mismas, que ayude a buscar y corregir errores. **k)** La solución debe tener la capacidad de asignar politicas de acceso basadas en url, nombres de usuario, aplicaciones, dominios y no solamente por dirección ip. **l)** Incluir un contador de acceso para cada regla de seguridad o generar un reporte que presente la utilización de cada una de las reglas. **m)** Los componentes de la solución deben ser accesibles a través de SSH o de interfaz Web usando SSL **n)** La plataforma debe ser capaz de construir políticas sin importar si estas referencian a objetos o servicios IPv4 o IPv6. **o)** Tener la capacidad de forma nativa en tiempo real, de dar información sobre el estado de los dispositivos administrados (conectividad, nivel cpu, tráfico de red) e ilustrar de forma gráfica al menos eventos como la conexión de usuarios remotos vía VPN, estado de los túneles IPSEC y tráfico más común sobre las interfaces (monitor), IPS, ANTIBOT, mayores intentos de conexiones entrantes y salientes. **p)** Configurar restricciones por direcciones IP (direcciones individuales, rangos, nombres de equipos) que pueden tener control sobre la consola de administración central. **q)** Debe tener la posibilidad de definir expiración de reglas de forma automática, por fecha y hora. **r)** Configurar restricciones por geolocalización. **s)** La autenticación de administradores a las consolas de gestión de políticas debe configurarse por lo menos con alguno de los siguientes mecanismos: contraseña o certificados digitales propios de la solución de seguridad o sistemas RADIUS. **t)** Configurar roles de administración. **u)** Permitir la creación de filtros en los logs basados en cualquiera de las características del evento, tales como: firewall virtual o físico, IP de origen y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, país de origen o destino, entre otros. **v)** Presentar la distribución de eventos por países. **w)** Permitir agrupar los eventos en base a cualquier característica de estos, pudiendo agrupar en varios niveles. **x)** Permitir realizar búsquedas dentro del listado de eventos. **y)** Las consolas de gestión deben incluir las funcionalidades que permitan la consolidación de

	registros (logs) y provea de mecanismos de correlación y generación de reportes. **z)** Incluir reportes predefinidos con los eventos detectados en la última hora, día, semana y mes. Incluyendo al menos Eventos top, Orígenes top, Destinos top, Servicios top, Orígenes top con sus eventos top, Destinos top con sus eventos top y Servicios top con sus eventos top y estado de las VPN. **aa)** Permitir la programación de reportes para que se ejecuten automáticamente para extraer información en periodos regulares de tiempo (diarios, semanales y mensuales). También debe permitir al administrador ver la fecha y horario en que empezará a generar el reporte agendado. **bb)** Soportar los siguientes formatos de reportes: HTML, CSV **cc)** Permitir la distribución automática de los reportes por correo electrónico, subiéndolos en un servidor FTP/Web y utilizando un script externo para la distribución del reporte. **dd)** Proveer reportes de información consolidada sobre al menos: i. Top de eventos por origen ii. Top de eventos por destino iii. Eventos por fecha. iv. Eventos por semana. v. Top de eventos por producto vi. Top de eventos por servicios. vii. Severidad viii. Producto ix. Geolocalización x. Cumplimiento de las regulaciones requeridas por Ministerio. **ee)** Los reportes deben poder generarse en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real. **ff)** Detectar ataques de denegación de servicio, correlacionando eventos de todas las funcionalidades solicitadas. **gg)** Debe soportar la integración con Active Directory mínimo con Microsoft 2012 R2 y Microsoft 2016 independiente sí es IPv4 o IPv6. **hh)** La solución debe ser capaz de adquirir la identidad de los usuarios, desde un Directorio Activo Microsoft 2012 R2 y Microsoft 2016 sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft. **ii)** La solución debe permitir la generación de backup y restauración de las configuraciones, políticas y logs permitiendo al administrador programar la realización de los backups en el tiempo deseado. **jj)** Los backups deben poderse almacenar localmente y transferir automáticamente vía FTP o SCP a un equipo que defina el Ministerio.
5.	**TRANSFERENCIA DE CONOCIMIENTOS** Durante la ejecución del contrato, se debe brindar una (1) transferencia de conocimientos certificada en la última versión del software instalado de acuerdo con los estándares establecidos por el fabricante

	Check Point, para tres (3) ingenieros de la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público, en la cual se provea conocimientos específicos de las funcionalidades requeridas en cuanto a administración, configuración y operación de consolas de gestión de firewall en alta disponibilidad, administración de identidades, virtualización, VPN, IPS, Threat Prevention y Antibot. La transferencia de conocimiento deberá brindarse cumpliendo con lo siguiente: **a)** Tener una intensidad horaria de mínimo de 40 horas **b)** Ser dictada por personal certificado por el fabricante de las soluciones ofertadas y en centros de entrenamiento autorizados por casa matriz. **c)** Disponer de equipos para realizar laboratorios prácticos **d)** Entregar el correspondiente material y certificaciones de asistencia con intensidad horaria a cada uno de los asistentes.
6.	**GARANTÍA Y SOPORTE TÉCNICO**
6.1.	La garantía consiste en mantener todos los equipos y sus componentes de hardware y software en perfecto estado de funcionamiento mediante reemplazo y/o reparación y/o actualización del componente defectuoso por parte del contratista por tres (3) años contados a partir de la generación del acta de recibo a satisfacción de los equipos descritos en el numeral 1.1 del presente Anexo. **a)** Los equipos reemplazados y las reparaciones a los mismos que se requieran con ocasión de los servicios de mantenimiento o soporte técnico deberán contar con garantía del fabricante Check Point a través del contratista durante el período de garantía ofrecido. **b)** Las partes y reparaciones que se requieran para restablecer la funcionalidad de los equipos deberán ser nuevas y originales en todos los casos y proporcionadas por el Contratista. **c)** Debe incluir, mano de obra, reemplazo de partes y actualización de versiones del software liberadas por el fabricante, previa autorización del Ministerio de Hacienda y Crédito Público. El proveedor debe considerar un período de estabilidad de la implementación de las consolas, el cual tendrá vigencia hasta la fecha de finalización del contrato que se suscriba como resultado del presente proceso. Durante este período de estabilización deberá: **a)** Atender y solucionar los incidentes del sistema operativo, de los productos de software instalados y del hardware de la solución provista, así como la aplicación de los correctivos necesarios para restablecer y preservar el buen funcionamiento de las mismas. **b)** Brindar técnica los requerimientos de garantía 7x24 mediante la atención vía telefónica, acceso remoto, por correo electrónico o en sitio a solicitud del Ministerio. **c)** Permitir el registro en las herramientas de soporte técnico del fabricante Check Point de casos de soporte y realizar el seguimiento a los casos abiertos directamente o escalados a través del contratista. **d)** Implementar las directrices recomendadas por el fabricante o el contratista o el entorno tecnológico, ante el surgimiento de debilidades o amenazas de seguridad detectadas. La atención se prestará bajo las siguientes condiciones:

	a) Garantizar la recuperación estable de los servicios en máximo cuatro (4) horas, contados a partir del registro del incidente, tiempo durante el cual puede proporcionar una solución provisional siempre y cuando no se presente deterioro de la calidad de los servicios implementados. **b)** Las partes y reparaciones que se requieran para restablecer la funcionalidad de los equipos deberán ser nuevas y originales en todos los casos y proporcionadas por el Fabricante.
7.	**MEJORAS CONTINUAS DEL SERVICIO** El Contratista al identificar oportunidades de mejora que conlleven a operaciones más eficaces las deberá incorporar al servicio, previo acuerdo con el Ministerio, a través del supervisor del contrato.
8.	**CONFIDENCIALIDAD** El diagrama de infraestructura presentado por el contratista para la implementación la validación de las configuraciones, las actividades de configuraciones finales realizadas para la implementación,; la atención de incidentes que realicen los expertos; así como; la información que sea entregada por el Ministerio dentro de las actividades objeto del contrato serán tratados por el Contratista en forma confidencial, adhiriéndose a las políticas de seguridad y de terceros de la Entidad.
9.	**ACREDITACIÓN E IDENTIFICACIÓN DEL PERSONAL AUTORIZADO** El Contratista, deberá acreditar e identificar previamente al personal autorizado ante el Ministerio para que le sea permitido el acceso a las instalaciones y a la solución objeto del Contrato.
10.	**RECURSO HUMANO** Para la ejecución del contrato el contratista prestará el servicio de soporte y mantenimiento técnico con mínimo el recurso humano que se relaciona a continuación:

DESCRIPCIÓN	EXPERIENCIA REQUERIDA
Ingeniero cuyo núcleo básico de conocimiento sea: • Ingeniería de Sistemas, Telemática y Afines o • Ingeniería Eléctrica y Afines o • Ingeniería Electrónica, Telecomunicaciones y Afines Debe contar con los siguientes certificados: • Check Point Certified Security Master CCSM • Check Point Certified Troubleshooting (Specialist Acreditation)	Experiencia mínima certificada de 2 años en implementación o soporte o mantenimiento o instalación o administración de soluciones de firewall Check Point.

El OFERENTE deberá aportar con su oferta los siguientes documentos:

a. Hoja de Vida
b. Copia de la cédula de ciudadanía
c. Copia de los títulos académicos y/o Acta de Grado

	d. Certificación de vigencia de la matricula profesional expedida por la Entidad que regule el ejercicio de su profesión. e. Autorización de trabajo para ejercer la profesión en Colombia, en el caso de que aplique. f. Certificado Check Point Certified Security Master CCSM Y Check Point Certified Troubleshooting (Specialist Acreditation) g. Certificaciones que acrediten la experiencia. Las certificaciones de experiencia del recurso humano deberán ser emitidas por la firma o entidad contratante y contener como mínimo la siguiente información: 1. Nombre o razón social de la firma o entidad que emite la certificación 2. Nombre e identificación de la persona a la que se está certificando 3. Actividades y/u obligaciones específicas realizadas. 4. Período de ejecución indicando fechas de inicio y terminación. Por otra parte, en los casos en los que no se determine la información del día de manera exacta, se tomará el día quince (15) del mes como fecha de inicio y/o de terminación. El profesional ofrecido por el OFERENTE no podrá ser objeto de cambio durante la ejecución del contrato sin previa autorización y verificación por parte del Supervisor del contrato. Si durante la ejecución del contrato se da el caso de cambio del recurso humano, el contratista remitirá máximo 5 días hábiles anteriores a la fecha prevista para el cambio, para aprobación del supervisor del contrato: la hoja de vida con sus respectivos soportes de experiencia, certificación de vigencia de la Matrícula o Tarjeta Profesional expedida por la Entidad que regule el ejercicio de su profesión y la certificación de Check Point vigente, del ingeniero propuesto para dicho cambio. El perfil del nuevo profesional no podrá ser inferior al perfil del profesional objeto de cambio y deberá acreditarse de la forma prevista en el párrafo anterior. En todo caso el Ministerio de Hacienda y Crédito Público, se reserva la facultad de solicitar a través del supervisor del contrato, el cambio del profesional en caso de no existir entera satisfacción acerca del desarrollo de las actividades a su cargo. Lo anterior será verificado por el supervisor designado por el competente contractual al momento de la suscripción del contrato.

ANEXO No. 2

COTIZACIÓN ECONÓMICA

Numeral	Descripción	Cantidad	Valor unitario incluido IVA	Valor total incluido IVA
ITEM 1	Consolas en alta disponibilidad para la gestión de las soluciones de firewalls perimetrales de SIIF Nación.	2		
	Soporte y garantía con fabricante Check Point	N.A.		
	INSTALACION E IMPLEMENTACION			
			TOTAL ITEM 1	
ITEM 2	Consolas en alta disponibilidad para la gestión de las soluciones de firewalls perimetrales del Ministerio de Hacienda y Crédito Público.	2		
	Soporte y garantía con fabricante Check Point	N.A.		
	INSTALACION E IMPLEMENTACION			
			TOTAL ITEM 2	
			VALOR TOTAL INCLUIDO IVA	

ANEXO No. 3
INFORMACIÓN ADICIONAL

El cotizante, corresponde a alguna de las siguientes categorías:

	SI	NO
MICRO EMPRESA		
PEQUEÑA EMPRESA		
MEDIANA EMPRESA		

Relacione contratos celebrados relacionados con el objeto cotizado, en los cinco (5) últimos años con otras Entidades Estatales y/o Privadas (número y fecha del contrato, nombre entidad contratante).

No. del Contrato	Fecha del Contrato	Objeto del Contrato	Nombre Entidad Contratante

INFORMACIÓN RELACIONADA CON EMPRENDIMIENTOS Y EMPRESAS DE MUJERES

Por favor diligenciar sí el cotizante se encuentra en alguna de las siguientes definiciones:

DEFINICIONES	SI
Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica pertenezcan a mujeres y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección	
Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel. Entendiéndose como empleos del nivel directivo aquellos cuyas funciones están relacionadas con la dirección de áreas misionales de la empresa y la toma de decisiones a nivel estratégico.	

En este sentido, serán cargos de nivel directivo los que dentro de la organización de la empresa se encuentran ubicados en un nivel de mando o los que por su jerarquía desempeñan cargos encaminados al cumplimiento de funciones orientadas a representar al empleador.	
Cuando la persona natural sea una mujer y haya ejercido actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior a la fecha de cierre del proceso de selección.	
Asociaciones y cooperativas, cuando más del cincuenta por ciento (50%) de los asociados sean mujeres y la participación haya correspondido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.	

INFORMACIÓN PARA EL FOMENTO DE SUJETOS EN ESPECIAL PROTECCIÓN CONSTITUCIONAL.

El cotizante cuenta con alguno de los siguientes grupos poblacionales, para la provisión de bienes o servicios para la ejecución del objeto cotizado:

GRUPOS POBLACIONALES	SI
Población en pobreza extrema	
Desplazados por la Violencia	
personas en proceso de reintegración o reincorporación	
Víctima del conflicto armado interno	
Mujeres cabeza de familia	
Adultos mayores	
Personas en condición de discapacidad	
Comunidades Indígenas, negra, afrocolombiana, raizal, palanquera, Rom o gitanas	
Otros sujetos de especial protección constitucional	

PROVEEDOR

Nombre o Razón Social del Cotizante _____
Nombre del Representante _____
Nit o Cédula de Ciudadanía No. _____ de_____
Dirección _____
Ciudad _____
Teléfono _____
Fax _____
Correo electrónico _____