Nombre de la compra:	**Adquisición en modalidad de llave en mano de equipos de protección de ataques tipo DDoS – AC 79777**
Fecha:	**5-11-2020**

I. Objetivo de la Compra

La Empresa de Servicios Públicos de Heredia (ESPH) requiere del servicio de contratación en modalidad llave en mano, para la adquisición e implementación de equipos para protección de ataques tipo DDoS.

II. Requerimiento de Materiales

En la siguiente tabla detallar la lista de los materiales a adquirir en la compra:

Item	Cantidad	Código del artículo *	Descripción
1	1	500-010-093-000	Servidor de mitigación de ataques DDoS
2	1	000-000-000-000	Licenciamiento
3	1	000-000-000-000	Servicios de implementación
4	1	000-000-000-000	Soporte

* *Según el Almacén de la ESPH, S.A.*

III. Especificaciones Técnicas

A continuación, se indican las especificaciones técnicas que debe tener la solución para protección de ataques tipo DDoS (Ataque de denegación de servicio), requerida por la ESPH:

Ítem 1: Servidor de mitigación de ataques DDoS

1.1 ARQUITECTURA

1.1.1 La solución debe integrar un dispositivo de protección dedicado en las premisas que se detallan y no una función con licencia en un Firewall, Manejador de Ancho de Banda o un en Balanceador de carga.

1.1.2 La solución de mitigación de ataques DDoS se debe integrar a la red de forma transparente en capa 2.

1.1.3 Debe soportar despliegues fuera de línea usando puertos SPAN o puertos mirror.

1.1.4 Cada equipo debe tener la siguiente configuración de interfaces para su integración a la red:

1.1.4.1 6 interfaces de Cobre 1000BaseT con al menos 2 módulos de bypass externos de la misma marca para proteger 3 segmentos de red que se

destruye de la siguiente manera: proteger 2 segmentos de red con Bypass y protección de 1 segmento de red sin Bypass.

1.1.4.2 2 interfaces de Fibra a 10GBase LR con al menos 1 módulo de bypass externo de la misma marca para proteger 1 segmento de red monomodo a 10G.

1.1.5 Se debe de incluir los SFPs necesarios,

1.1.6 La solución de mitigación debe contar con las siguientes interfaces totales para crecimiento futuro. Solo se deben incluir los SFPs mencionados en el ítem anterior

1.1.6.1 24 (SFP+) que pueden ser instalados como GE / 10GE

1.1.7 El dispositivo debe incluir al menos dos interfaces de gestión (Management Ports) y administración por consola RJ45.

1.1.8 La solución de mitigación de ataques DDoS debe soportar al menos los siguientes tipos de túneles: VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP.

1.1.9 La solución de mitigación de ataques DDoS debe soportar IPv4 e IPv6.

1.1.10 La solución de mitigación de ataques DDoS debe soportar un número ilimitado de sesiones concurrentes de ataque.

1.1.11 La solución de mitigación de ataques DDoS debe incluir doble fuente de poder hot swappable.

1.1.12 La solución deberá soportar “Jumbo Frame”.

1.2 CAPACIDAD

1.2.1 La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de al menos 4Gbps por equipo.

1.2.2 La solución de mitigación de ataques DDoS debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 12Gbps por equipo.

1.2.3 La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 20 Gbps por equipo.

1.2.4 La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 25 MPPS por equipo.

1.2.5 La solución de mitigación de ataques DDoS debe tener una latencia menor a 60 microsegundos.

1.3 FUNCIONALIDADES DE DETECCIÓN Y MITIGACIÓN DE ATAQUES

1.3.1 La solución debe proteger contra al menos las siguientes anomalías de tráfico:

- Checksum incorrecto de IPV4.
- Tamaño de Cabecera capa invalido.
- TTL igual a 0.
- Cabecera IPV6 inconsistente.
- Límites de salto IPV6 alcanzados.
- Protocolo Capa 4 no soportado.
- TCP flags invalido.
- Tamaño de cabecera UDP invalido.
- Dirección de origen o destino igual al Local Host.
- Dirección de origen igual a la dirección de destino.
- Puerto Capa 4 de origen o destino igual a cero.
- Cebera de GRE invalida
- Versión GRE Incorrecta.

1.3.2 La solución debe operar a través de políticas de seguridad con distintas configuraciones de detección y mitigación de acuerdo a los objetos protegidos.

1.3.3 Las políticas de seguridad se podrán habilitar o deshabilitar individualmente.

1.3.4 Las políticas de seguridad se podrán configurar en modo reporte o en modo bloqueo.

1.3.5 Las configuraciones de detección y mitigación dentro de una política de seguridad específica, se podrán configurar individualmente en modo reporte o en modo bloqueo.

1.3.6 La solución debe contar con análisis de comportamiento de red para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos las siguientes inundaciones de tráfico:

- Inundación de red UDP.
- Inundación de red ICMP.
- Inundación de red IGMP.
- Inundación de red TCP con flag SYN.
- Inundación de red TCP con flag RST.
- Inundación de red TCP con flag ACK.
- Inundación de red TCP con flag PSH.
- Inundación de red TCP con flag FIN.
- Inundación de red TCP con flag SYN y ACK.
- Inundación de red TCP flag FRAG.
- Inundación de red UDP con flag FRAG.

1.3.7 La solución debe aprender acerca del tráfico y configurar automáticamente las líneas bases de tráfico y thresholds de ataques.

1.3.8 La solución debe correlacionar parámetros que varíen con la tasa de tráfico con parámetros que no varíen con la tasa de tráfico para determinar la condición de ataque.

1.3.9 La solución debe permitir configurar un umbral de ancho de banda de supresión de aprendizaje, para evitar que las líneas bases se distorsionen en bajo tráfico.

1.3.10 La solución debe crear y aplicar automáticamente y en tiempo real una firma para detener los ataques en capa de red.

1.3.11 La solución debe proteger contra ataques de tipo ráfaga (burst attacks) identificando que una nueva ráfaga de tráfico pertenece a una firma en tiempo real previamente creada.

1.3.12 La solución debe incluir un mecanismo de prevención de overblocking de tráfico el cual valide y refresque la firma, si se está bloqueando más tráfico del debido.

1.3.13 La solución debe permitir especificar un límite de tasa de tráfico que servirá como un método alternativo automático a la firma en tiempo real de red.

1.3.14 La solución de mitigación de ataques DDoS debe incluir un mecanismo de límite de conexiones TCP y sesiones UDP que cumpla con las siguientes características:

- La solución debe contar el número de conexiones TCP o sesiones UDP abiertas por cliente, por servidor, o por la combinación de cliente y servidor.
- La solución debe permitir descartar los paquetes que pasen el límite establecido.
- La solución debe permitir suspender el tráfico por un tiempo determinado si este pasa del límite establecido.

1.3.15 La solución de mitigación de ataques debe incluir un mecanismo que haga seguimiento y bloquee paquetes que superen una tasa de PPS en sesiones definidas.

1.3.16 La solución debe incluir protección contra ataques DDoS de inundación de paquetes fuera de estado.

1.3.17 La solución debe incluir protección contra ataques DDoS de tipo SYN Flood

1.3.18 La protección contra ataques SYN Flood a través del seguimiento de paquetes SYN enviados a cada IP Destino y Puerto.

1.3.19 La protección de SYN Flood debe prevenir contra ataques de tipo Spoofed-SYN-flood que vayan dirigidos a múltiples puertos destinos, a través del seguimiento de paquetes SYN enviados a toda la red configurada en la política.

1.3.20 La protección de SYN Flood debe contar con al menos dos métodos de autenticación TCP: ACK Fuera de Secuencia y Proxy Transparente

1.3.21 La protección de SYN Flood, para los protocolos http y https, debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script.

1.3.22 La solución permitirá al operador crear filtros de tráfico.

1.3.23 Los filtros de tráfico deben permitir como mínimo seleccionar los siguientes criterios para hacer match al tráfico:
- Red de Origen
- Red de Destino
- Puerto Origen
- Puerto Destino
- Protocolo
- Tamaño del Paquete
- Flags TCP
- Time to Live (TTL)
- Número de Secuencia TCP
- Type of Service (ToS) / DSCP
- Fragment Offset
- Fragment ID

1.3.24 Los filtros de tráfico deben permitir crear expresiones regulares para filtrar tráfico de acuerdo al payload de los paquetes recibidos.

1.3.25 Los filtros de tráfico deben permitir configurar límites de tráfico en PPS o bps, sobre el tráfico que haga match con los criterios definidos.

1.3.26 La solución debe contar con protección de ataques DDoS DNS basada en análisis de comportamiento para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos los siguientes tipos de inundaciones de Queries DNS: A, AAAA, MX, PTR, Test, SOA, NAPTR, SRV, Other.

1.3.27 La solución debe aprender acerca del tráfico DNS y configurar automáticamente las líneas bases de tráfico y thresholds de ataques.

1.3.28 La solución debe permitir configurar un umbral de QPS de supresión de aprendizaje, para evitar que las líneas bases se distorsionen en bajo tráfico.

1.3.29 La solución debe aprender e incluir en una lista blanca el TOP de FQDNs en el tráfico DNS.

1.3.30 La lista blanca con el TOP de FQDNs se podrá exportar y se podrán añadir entradas a la lista de forma manual.

1.3.31 La solución debe crear y aplicar automáticamente y en tiempo real una firma para detener el ataque de DNS.

1.3.32 En condición de ataque DDoS, la solución debe bloquear todo el tráfico hacia el DNS que este fuera del complaince del protocolo DNS.

1.3.33 La solución debe incluir un mecanismo de reto y respuesta en DNS para minimizar falsos positivos.

1.3.34 La solución debe mitigar inundaciones de DNS recursivas (inundaciones de dominios aleatorios) bloqueando el tráfico que haga match con la firma en tiempo real creada, mientras permite el tráfico en la lista de FQDNs aprendida.

1.3.35 La protección de ataques DDoS DNS de la solución propuesta debe basarse únicamente en el tráfico entrante (Ingress-Only o Inbound).

1.3.36 La protección de ataques DDoS DNS debe mitigar ataques de tipo amplificación o reflexión de DNS.

1.3.37 La protección de ataques DDoS DNS debe mitigar ataques de tipo Brute Force de DNS

1.3.38 La solución debe permitir crear reglas de listas negras y listas blancas, incluyendo al menos los siguientes parámetros de clasificación:

- Red Origen
- Puerto Origen
- Red Destino
- Puerto Destino
- Protocolo

1.3.39 La solución de mitigación de ataques DDoS debe incluir un mecanismo de protección contra escaneos de puertos TCP, UDP e ICMP.

1.3.40 La protección contra escaneos debe funcionar a través de análisis de comportamiento y el nivel de sensibilidad de la protección debe ser configurado por el operador.

1.3.41 La protección contra escaneos debe tener la capacidad de crear listas blancas de direcciones IP origen y puertos.

1.3.42 La protección contra escaneos debe generar una firma en tiempo real para bloquear el escaneo de puertos realizado.

1.3.43 La solución de mitigación de ataques DDoS debe incluir una protección basada en firmas de ataques conocidos que permita al menos mitigar los siguientes tipos de ataques:

- Inundaciones TCP, UDPe ICMP conocidas
- Herramientas de ataques conocidas disponibles en Internet
- Inundaciones de ataques conocidos creados por bots
- Vulnerabilidades en los servidores: Web, Mail, FTP, SQL, DNS, SIP
- Troyanos y backdoors
- Gusanos y Virus
- IRC Bots
- Spyware
- Phishing
- Anonymizers

1.3.44 La protección basada en firmas de ataques conocidos debe incluir grupos de firmas preconfigurados para ser aplicados en las políticas.

1.3.45 La protección basada en firmas de ataques conocidos debe permitir crear grupos de firmas por elementos comunes y aplicar los grupos de firmas en las políticas.

1.3.46 La protección basada en firmas debe permitir a los operados crear sus propias firmas.

1.3.47 La solución de mitigación de ataques DDoS debe incluir una suscripción para actualización de la protección basada en firmas.

1.3.48 La solución de mitigación de ataques DDoS debe incluir una suscripción que permita el bloqueo por geolocalización.

1.3.49 La protección de geolocalización debe permitir la configuración de un perfil de bloqueo por países y asignarlo a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas.

1.3.50 La protección de geolocalización debe permitir la configuración de un perfil para permitir países seleccionados y asignarlo a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas.

1.3.51 La solución de mitigación de ataques DDoS debe incluir una lista de IP de mala reputación productos del centro de investigación del fabricante, que será actualizada periódicamente.

1.3.52 La lista de IP debe incluir al menos las siguientes categorías:

- Atacantes Activos: Direcciones IP que han sido correlacionados y se han determinado como maliciosas.
- Tor Exit Nodes: Una IP que es un Tor Exit Node, sin importar si ha participado o no en actividades de ataques.
- Web Attackes: Una IP que ha hecho intentos de violaciones Web.

1.3.53 Para cada una de las categorías listadas se podrá configurar al menos las siguientes acciones: Bloqueo, Bloqueo y Reporte, Bypass.

1.3.54 La lista de IP maliciosas, en conjunto con las acciones configuradas por categorías, debe aplicarse sobre cada política de seguridad.

1.4 CONSOLA DE GESTIÓN

1.4.1 Se debe incluir una consola de gestión debe ser del tipo Virtual Appliance y deberá poder instalarse sobre Hyper-V o Vmware ESXI 5 o superior en los servidores de la entidad.

1.4.2 La consola de gestión debe soportar la administración y monitoreo de todos los Mitigadores que hacen parte de la propuesta de forma centralizada.

1.4.3 La consola de gestión permitirá asignar roles de administración y monitoreo de seguridad por cada uno de los equipos administrados.

1.4.4 La consola de gestión debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.

1.4.5 La consola de gestión debe soporta autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+.

1.4.6 La consola de gestión debe permitir la configuración de NTP.

1.4.7 La consola de gestión deberá permitir el acceso por REST API. Todas las operaciones que puedan realizarse a través de esta API deben estar completamente documentadas.

1.4.8 La consola de gestión deberá permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se realizan sobre los equipos.

1.4.9 "La consola de gestión debe soportar al menos las siguientes alertas de auditoria y sistema:

- Alarmas de servidor.
- Alarmas generales del dispositivo (fan, CPU)
- Mensajes de auditoría

1.4.10 La consola de gestión debe permitir configuración de alertas a servidores de syslog y snmp externos.

1.4.11 La consola de gestión debe permitir visualizar la utilización de CPU de los dispositivos administrados.

1.4.12 La consola de gestión debe contar con una funcionalidad que permita la captura de paquetes que ingresan y salen del equipo. Estos archivos deberán estar en formato CAP y deben poder descargarse.

1.4.13 La consola de gestión debe permitir definir al menos los siguientes parámetros dentro de la captura: Duración, número de paquetes a Capturar, IP origen, IP Destino, Protocolo

1.4.14 La consola de gestión debe permitir creación de tareas calendarizadas de backup de los dispositivos administrados.

1.4.15 La consola de gestión permitirá guardar los backups localmente o enviarlos a un repositorio externo a través de SCP, SFTP o SSH.

1.4.16 La consola de gestión debe permitir creación de tareas calendarizadas para las actualizaciones de seguridad del dispositivo.

1.4.17 Desde la consola de gestión se podrá realizar la actualización de la versión principal de los dispositivos administrados.

1.4.18 Desde la consola de gestión se podrán administrar distintas versiones de los dispositivos, teniendo la chance de un rollback de versión en case de necesitarse

1.4.19 La consola de gestión debe permitir la administración de múltiples dispositivos, pudiendo realizar configuración simultánea en varios dispositivos.

1.4.20 La consola de gestión debe permitir la creación de scripts y flujos de trabajo para automatizar tareas de configuración recurrentes.

1.4.21 La consola de gestión debe permitir la comparación de la configuración entre dos dispositivos.

1.4.22 La consola de gestión debe permitir la comparación de la configuración entre un dispositivo y un backup determinado.

1.5 MONITOREO DE SEGURIDAD

1.5.1 La consola de gestión debe mostrar en tiempo real los eventos de seguridad detectados por la solución de mitigación de ataques DDoS.

1.5.2 El monitoreo en tiempo real de los ataques debe mostrar el estado actual de la infraestructura indicando claramente si hay o no un ataque en curso.

1.5.3 El monitoreo en tiempo real debe mostrar estadísticas gráficas del tráfico total entrante y saliente en bits por segundo y paquetes por segundo.

1.5.4 El monitoreo en tiempo real debe mostrar estadísticas gráficas de las conexiones por segundo y conexiones concurrentes recibidas.

1.5.5 Bajo ataque, el monitoreo en tiempo real debe mostrar por política o objeto protegido al menos la siguiente información:

- Tráfico total entrante.
- Tasa de ataque y tasa de paquetes descartados en bps.
- Tasa de ataque y tasa de paquetes descartados por cada tipo de mitigación aplicada.

1.5.6 Mitigaciones aplicadas y estadísticas gráficas del ataque que permitan validar el impacto de las contramedidas.

1.5.7 El módulo de analítica debe permitir tener visibilidad de geolocalización, pudiendo visualizar al menos lo siguiente:

- Top de geolocalizaciones atacantes no bloqueadas.
- Geolocalizaciones bloqueadas temporalmente.
- Geolocalizaciones bloqueadas de forma permanente.
- Geolocalizaciones permitidas.

1.5.8 Dentro de las funcionalidades de geolocalización, la consola debe permitir el bloqueo temporal de geolocalizaciones seleccionadas.

1.5.9 El monitoreo en tiempo real debe mostrar estadísticas gráficas de tráfico por política de seguridad u objeto protegido, para al menos los siguientes tipos de tráficos: SYN, SYN-ACK, RST, FIN-ACK, TCP Fragmented, UDP Fragmented, UDP, ICMP, IGMP

1.5.10 El monitoreo en tiempo real debe mostrar estadísticas gráficas de tráfico por política de seguridad u objeto protegido, para al menos los siguientes tipos de queries DNS: Tipo A, AAAA, MX, TXT, SOA, SRV, PTR, NAPTR.

1.5.11 El monitoreo en tiempo real debe mostrar estadísticas gráficas de tráfico por cada servidor https protegido.

1.5.12 El monitoreo en tiempo real debe incluir dashboard con al menos la siguiente información:

- Top de Ataques.
- Top de Ataques por Ancho de Banda.
- Top de los Destinos y Orígenes de los Ataques.
- Top de Ataques por Protocolo.
- Top de Ataques por Acción de Mitigación.

1.5.13 La consola de Gestión debe incluir un Dashboard en donde se muestre el impacto de las listas de mala reputación configuradas en la solución de mitigación de ataques DDoS.

1.5.14 El Dashboard de IP maliciosas debe incluir el TOP de eventos, TOP de paquetes y TOP por volumen de tráfico, por al menos los siguientes críterios:

- Geolocalización
- Actividad Maliciosa
- Direcciones IP Origen
- Línea de tiempo

1.5.15 El Dashboard debe permitir modificar el tiempo de muestra datos con una profundidad máxima de 3 meses.

1.6 ALERTAS Y REPORTES

1.6.1 La consola de gestión debe permitir generar reportes históricos de los ataques detectados y mitigados por la solución.

1.6.2 La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.

1.6.3 La consola de gestión debe permitir configurar un rango de tiempo de hasta 1 año para la generación de reportes históricos.

1.6.4 Debe soportar formatos PDF, CSV y HTML para los reportes históricos.

1.6.5 Debe permitir la personalización del logo de la entidad en los reportes.

1.6.6 Debe permitir escoger los mitigadores y las políticas de seguridad específicas sobre los cuales se extraerá el reporte.

1.6.7 La consola de gestión debe permitir personalizar el contenido de los reportes con mínimo las siguientes estadísticas:

- Top de Ataques
- Top de Ataques por Ancho de Banda
- Top de los Destinos y Orígenes de los Ataques
- Top de Ataques por Protocolo
- Top de Ataques por Acción de Mitigación
- Estadística gráfica de ancho de banda
- Tasa de conexión por segundo
- Estadísticas de Conexiones concurrentes

1.6.8 La consola de gestión debe permitir búsquedas de eventos de seguridad a través de la definición de criterios de búsqueda.

1.6.9 La consola de gestión debe permitir anidar múltiples criterios a través de expresiones regulares

1.6.10 Desde la consola de gestión se deben enviar alertas de ataques

1.6.11 Debe permitir escoger los mitigadores y las políticas de seguridad específicas sobre los cuales se realizará la configuración de la alerta

1.6.12 Desde la consola de gestión se podrá personalizar el tipo de alertas que se enviarán a través de la creación de expresiones regulares.

1.6.13 Desde la consola de gestión se podrá configurar la severidad de la alerta.
1.6.14 El Oferente deberá suministrar toda la documentación técnica que permita verificar las características de los equipos y componentes ofertados. La documentación podrá ser únicamente en idioma español o inglés.

Ítem 2: Licenciamiento

2.1 El oferente debe incluir en su oferta, todo el licenciamiento necesario para que la solución funcione de forma adecuada.
2.2 El licenciamiento debe quedar a nombre de la Empresa de Servicios Públicos de Heredia.
2.3 Debe tener una vigencia de 5 años
2.4 Al momento de la implementación, debe entregarse documentación a la ESPH, que demuestre la vigencia de todo el licenciamiento adquirido.
2.5 El licenciamiento se contratará a 5 años, por lo que el oferente debe indicar claramente en su oferta el costo de éste en cada uno de los años.

Ítem 3: Servicios de implementación

3.1 El oferente será responsable de la instalación y configuración completa de todos los componentes de hardware y software objeto de esta contratación (nuevos o ampliaciones), así como del soporte y mantenimiento de los mismos. Debe contemplar las pruebas que sean necesarias y su puesta en operación. El personal de ESPH debe participar durante todo el proceso de instalación, configuración, pruebas y puesta en operación.
3.2 El oferente debe contemplar en la instalación, el cableado de fibra óptica, el tiraje de estos cables y cualquier otro componente adicional que se requiera para el correcto funcionamiento del dispositivo, de acuerdo con las especificaciones de ESPH.
3.3 El oferente debe presentar una propuesta preliminar de las actividades a realizar para llevar a cabo la instalación y configuración de los componentes de esta contratación, incluyendo las pruebas de funcionamiento de los componentes de hardware y software involucrados, así como la interconectividad requerida con los equipos a ser aprovisionados al momento de la instalación, de manera que la instalación y configuración se realice a satisfacción de ESPH. Para ello debe proponer, a más tardar después de ocho días naturales a partir de la fecha de notificación de la orden de compra, un cronograma general de las actividades a realizar para llevar a cabo la instalación y configuración de los componentes de esta contratación. Dicho cronograma deberá ser aprobado por el administrador del contrato.

3.4 El oferente debe especificar los requerimientos físicos, eléctricos y ambientales requeridos para la correcta instalación de la configuración propuesta de los equipos objeto de esta contratación.
3.5 La instalación deberá ser efectuada por personal técnico de la empresa adjudicataria, debidamente certificados en los equipos adquiridos objeto de este cartel, en las instalaciones del ESPH, en coordinación y apoyo de funcionarios del ESPH.
3.6 El oferente debe realizar una revisión en el Centro de Cómputo designado por ESPH, para verificar que existan las condiciones de previstas eléctricas para la correcta instalación de los equipos ofertados, esta conexión eléctrica es desde el tablero principal de alimentación eléctrica provisto por el ESPH, previa coordinación con la parte técnica de un mínimo de dos días antes de la fecha efectiva de visita.
3.7 ESPH proporcionará toda la instalación eléctrica partiendo desde el tablero principal de alimentación eléctrica que posee en su Sala de Cómputo hasta el rack de esta contratación y proveer todos los componentes necesarios (tableros secundarios, cableado, conectores eléctricos, regletas). De modo que todos los componentes queden funcionando de forma óptima, de acuerdo con las especificaciones del fabricante y a plena satisfacción del ESPH.
3.8 El Oferente deberá suministrar toda la documentación técnica que permita verificar las características de los equipos y componentes ofertados y la forma en que fueron instalados. La documentación podrá ser únicamente en idioma español o inglés.

Ítem 4: Soporte

4.1 El oferente debe brindar soporte en un esquema 24x7x365 a la solución ofertada.
4.2 Debe poseer un protocolo de contacto tanto en horas hábiles como fuera de éstas.
4.3 Debe coordinar con fábrica los casos que corresponda para ser escalados y buscar una solución más especializada, en incidentes de mayor gravedad.
4.4 El oferente debe contar con una mesa de servicio donde poder hacer el ingreso de tickets.
4.5 El servicio de soporte se contratará a 5 años, por lo que el oferente debe indicar claramente en su oferta el costo de éstos en cada uno de los años.
4.6 Se debe brindar informes mensuales de la operación de la solución brindada, por toda la vigencia de 5 años.

IV. Requisitos de Admisibilidad

Por la importancia y el nivel de criticidad que este proyecto representa para ESPH y los servicios que se brindaran a terceros con la infraestructura a adquirir, la empresa deberá cumplir como mínimo con las siguientes especificaciones, la oferta que no cumpla quedará automáticamente descalificada del concurso sin posibilidad de presentar ningún tipo de apelación:

1. No se admitirán ofertas en consorcio o subcontratación de ningún tipo, tampoco se aceptarán ofertas parciales por líneas independientes, la empresa que presente su oferta deberá incluir la totalidad del requerimiento descrito en cada punto de este cartel.

2. No se admitirán ofertas cuyo tiempo de entrega supere los 22 días naturales.

3. Únicamente se aceptarán ofertas de empresas que estén debidamente radicadas en Costa Rica. El oferente deberá ser una empresa costarricense debidamente establecida y consolidada a su vez tenga presencia autorizada legalmente para operar en el territorio nacional y regional. Para ello deberá presentar la personería jurídica de la empresa.

4. La solución ofertada deberá entregarse bajo la modalidad “llave en mano”, y debe incluir la Instalación y configuración completa de la solución que se solicitan en este cartel y a satisfacción de la ESPH. El oferente debe cotizar la totalidad de los ítems

5. La empresa oferente deberá contar con al menos 5 años de brindar servicios de la marca del equipo ofertado, instalando, configurando y brindando soporte (sin recibir asistencia o sub-contratando al fabricante u otros proveedores) a soluciones de respaldo y recuperación similar a la ofertada. Debe presentar certificaciones de fábrica.

6. El oferente deberá aportar, además, una lista con al menos cinco (5) certificaciones de clientes en el mercado nacional, con los datos de nombre, teléfono y dirección de correo electrónico de al menos 5 implementaciones

exitosas de la misma marca de los componentes ofertados; los modelos de los equipos deberán corresponder a los mismos fabricantes de las soluciones ofertadas.

7. Se deberá aportar certificación del fabricante donde demuestre que es distribuidor directo (Tier 1) de la marca ofertada por los últimos 5 años, con un máximo de un (1) mes de haber sido emitida, dirigida a la ESPH.

8. El oferente debe tener un mínimo de diez (10) años de experiencia con la marca ofertada, demostrar que es representante autorizado por el fabricante y que cuenta con la certificación de más alto nivel del fabricante de la marca en Costa Rica. Para ello debe entregar una certificación del fabricante vigente, en el que haga constar todo lo anterior en territorio costarricense. Este documento deberá entregarse como parte de la oferta y debe tener un máximo de 30 días de emisión. El fabricante debe de indicar en la certificación explícitamente el concurso en cuestión y los ingenieros certificados.

9. El oferente debe contar con un equipo de trabajo y tener como mínimo:

- Un (1) gerente de proyecto, el cual deberá ser ingeniero, contar con las certificaciones del Project Management Professional (PMP), COBIT V.5 Foundation, ITIL Foundation V.3 e ISO 27001F, ser parte de la planilla de la empresa oferente, y ser ingeniero
- Dos (2) ingenieros especialistas que cuente con certificación del fabricante, estar incorporados al Colegio de Profesionales Informáticos y Computación CPIC, tener certificado en COBIT V.5 Foundation, ITIL Foundation V.3 e ISO 27001F y ser parte de la planilla del oferente.
- La importancia de que los ingenieros cuenten con certificaciones como COBIT V.5 Foundation, ITIL Foundation V.3 e ISO 27001F es con la finalidad de comprender el gobierno y la gestión de nuestra organización, así como referenciar mejores prácticas y recomendaciones para la correcta administración de servicios TI.
- Un Ingeniero certificado como Certified Information Systems Security Professional (CISSP), esto con el fin de certificar la formación en el área de seguridad de la información. El profesional deberá ser parte de la planilla de la empresa.

10. El oferente deberá entregar como parte de la oferta los currículums de los ingenieros indicados en la oferta y asignados al proyecto, se deberá presentar copia de los atestados (títulos) y currículos actualizados que certifiquen las calidades de cada uno y se demuestre documentalmente la idoneidad de éstos

para configurar e implementar la solución requerida. Todo el personal aportado para la ejecución de las tareas deberá ser parte de la planilla de la empresa oferente, para lo que se debe aportar las planillas de la Caja Costarricense del Seguro Social (CCSS) que así lo acrediten.

11. El oferente deberá especificar claramente la idoneidad (nombre, especialidad y grado académico) del personal que prestará la atención técnica. Es entendido que los estudios y la experiencia deben ser afines a la actividad de implementación a realizar, producto del objeto de este cartel.

12. El personal que se ofrezca en la implementación, deberá estar en todo momento para atender a ESPH, por lo cual no deberá incluirse personal que se encuentre destacado permanentemente en otras empresas, ello con el fin de asegurar una ejecución continua de la implementación.

13. Todas las certificaciones emitidas por terceros, en el exterior deben presentarse debidamente apostilladas.

14. Debe presentar los estados financieros auditados según las condiciones generales.

15. Debe presentar la estructura del precio, indicando en términos porcentuales y nominales; los costos directos, los costos indirectos y la utilidad.

16. El precio debe indicar claramente el detalle antes y después de impuestos

V. Documentos que Certifiquen la Calidad del Producto

Posterior a la implementación de los equipos, el proveedor adjudicado debe entregar una nota del fabricante, en donde se muestre el detalle de los equipos asignado a ESPH para responder por las obligaciones adquiridas por este cartel

VI. Condiciones de entrega e instalación

El equipo debe entregarse debidamente implementado en el Datacenter de la ESPH, ubicado en Heredia centro. El oferente deberá indicar en la oferta el plazo de entrega, el cual deberá expresarse en días naturales y contemplar incluso la instalación de los

equipos. El oferente indicará en días naturales un plazo de entrega de los equipos y un plazo de implementación.

VII. Garantía

El oferente deberá aportar una garantía de participación equivalente a un 1% del monto total ofertado, la cual será devuelta 30 días hábiles luego de la apertura de ofertas por parte de la ESPH.

El oferente adjudicado deberá aportar una garantía de cumplimiento equivalente a un 5% del monto total adjudicado, la cual se mantendrá vigente por todo el periodo de la contratación (5 años) y será devuelta 30 días hábiles después de que se realice el recibido a satisfacción por parte de la ESPH.

El oferente adjudicado deberá aportar una garantía de buen funcionamiento equivalente a un 5% del monto correspondiente al soporte de fábrica y soporte del oferente, la cual se mantendrá vigente por 4 meses posterior a los 5 años de la contratación.

VIII. Multas

Cuando exista atraso en la entrega total o parcial del bien y/o servicio adjudicado, conforme a las condiciones contratadas el adjudicatario deberá pagar a la ESPH, S.A. por concepto de multa el equivalente a un 2% sobre el valor total adjudicado, por cada día hábil que se mantenga dicha condición, hasta un máximo de 25% acumulado, todo de conformidad a las Condiciones Generales.

Acuerdo de Nivel de Servicio (SLA): El servicio de soporte y gestión de incidentes estará sujeto al acuerdo de servicio que se detalla en la siguiente matriz:

Matriz de SLA para Servicios Administrados

Descripción del Servicio	Tiempo SLA	Tiempo Penalidad	Multa
Primer Contacto Soporte por incidente	60 Minutos	> 60 Minutos	Por cada 5 minutos de retraso, 2,5% menos del Total Factura Mensual Hasta un 25% del monto mensual facturado.
Diagnostico Preliminar al Cliente	60 Minutos	> 60 Minutos	Por cada 10 Minutos de retraso, 2,5% menos del Total Factura Mensual Hasta un 25% del monto mensual facturado.
Tiempo Promedio Resolución Averías*	4 Horas	> 4 Horas	Por cada media hora de retraso, 5% menos Total de la Factura mensual, última media hora 2,5% hasta un 25% del monto mensual facturado.

*Se excluye de este periodo el tiempo requerido por el contratista para la sustitución de partes y/o equipos.
En caso de que el incidente se origine por un problema en el software atribuible al fabricante, el contratista informará el tiempo de resolución de acuerdo a la documentación técnica a proveer por parte del fabricante y el tiempo de resolución del incidente se extenderá.

IX. CONTRATO DE CONFIDENCIALIDAD.

La presente contratación, se formalizará mediante el giro de la orden de compra. Sin embargo, la adjudicataria, deberá suscribir un contrato de confidencialidad de previo a realizar la ejecución contractual, para lo cual, deberán coordinar con la Asesoría Jurídica de la ESPH.

X. TRANSFERENCIA DE CONOCIMIENTOS

La contratista, realizará una transferencia de conocimientos al personal de la ESPH, considerando lo siguiente:

- **Sitio de capacitación**: Modalidad virtual

-**Objetivos de capacitación**: Comprender la implementación, mantenimiento y operación del sistema de protección de ataques tipo DDoS ofertado.

- **Número de funcionarios ESPH a capacitar**: 2 en total

- **Tiempo mínimo de capacitación**: 32 horas

- Requisitos del capacitador: El capacitador deberá ser certificado en administración y operación del equipo ofertado.

Los oferentes deberán completar el formulario ESPHF-RH-077(1), denominado Catálogo de Curso para Proveedores de la ESPH, S.A.

XI. Tabla de Valoración para Comparar y Adjudicar

Las ofertas admitidas se compararán y adjudicarán artículo por artículo de acuerdo al sistema de puntajes que cada usuario desee utilizar, siendo la(s) oferta(s) seleccionada(s) para su adjudicación la que logre el mayor puntaje y cumpla con lo requerido por la Unidades Interesada y que a la vez favorezca los intereses de la ESPH, S.A.

Se establece el siguiente puntaje para la evaluación de ofertas

Concepto	Puntaje
a) Precio menor	70
b) Tiempo de entrega menor	20
c) Experiencia	10

A continuación, se determina la fórmula para calcular el puntaje obtenido según los rubros de la tabla anterior:

a) Precio

El oferente que cotice a menor precio, se le otorgarán 70 puntos, a cada artículo ofrecido se le calculará el puntaje de acuerdo con la siguiente fórmula:

$$P = X * (Pb/Po)$$

Donde:
P = Puntaje obtenido por la oferta en estudio.
X = Valor asignado proporcional al 100%.
Pb = Precio de la oferta de menor precio.
Po = Precio de la oferta en estudio.

b) Tiempo de entrega

Al oferente que ofrezca menor tiempo de entrega, se le otorgarán 20 puntos, a cada artículo ofrecido se le calculará el puntaje de acuerdo con la siguiente fórmula:

T= X* (Tb/To)
Dónde:

T = Puntaje obtenido por la oferta en estudio.
X = Valor asignado proporcional al 100%.
Tb = Período de la oferta de menor tiempo de entrega en días naturales.
To = Período de la oferta en estudio en días naturales.

c) Experiencia

Se otorgará hasta 10 puntos a los oferentes que demuestren tener más experiencia de la requerida como admisibilidad, y para ello se utilizará la siguiente tabla;

6 a 9 trabajos realizados demostrando experiencia brindando servicios de la marca del equipo ofertado, instalando, configurando y brindando soporte.	8
10 o más trabajos realizados demostrando experiencia brindando servicios de la marca del equipo ofertado, instalando, configurando y brindando soporte.	10

Para su validación, se utilizará la certificación solicitada en el punto IV.6 de requisitos de admisibilidad

XII. Forma de pago

La ESPH SA no realizará pagos por adelantado. La ESPH realiza el pago de facturas a 30 días naturales después del recibido a satisfacción de la implementación de los equipos.
El pago de la renovación del licenciamiento, soporte de fábrica y soporte del oferente, se realizará de forma anual a 5 años.

XIII. Formulario de Cotización

Ejemplo:

Ítem de Articulo	Nombre de Oferente	Fabricante	Marca	Modelo o Número de catálogo	Normas Aplicadas	Tiempo de Entrega en días naturales	Documentos que Certifiquen la Calidad del Producto	Observaciones
1								
2								

XIV. Consideraciones de Salud - Seguridad Ocupacional y Ambiente

El contratista está en la obligación de conocer y cumplir lo establecido en el documento Reglas de Calidad, Salud y Seguridad y Ambiente para Contratistas de la ESPH, S.A (el documento se encuentra en la página de la empresa www.esph-sa.com; en la cejilla de proveedores) y someterse a las inspecciones periódicas que la ESPH S.A. realice para verificar el cumplimiento del mismo.