



## DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

\*\*\*\*\*

**REF.:** ELABORACIÓN DE ESPECIFICACIONES  
TÉCNICAS PARA LA “ADQUISICIÓN DE EQUIPO  
FIREWALL PARA SEGURIDAD PERIMETRAL DE LA  
JUSTICIA ELECTORAL”.

### DICTAMEN TÉCNICO DTIC N° 01/2025

Asunción, 06 de enero de 2025

#### I) INTRODUCCIÓN

**El Director de la Dirección de Tecnologías de la Información y Comunicación, Lic. Fausto Von Streber,** a fin de dar cumplimiento a lo establecido en el Art. 40 –Documentaciones - de la Resolución DNCP N° 4401/2023, modificado por el Art. 12 de la Resolución DNCP N° 453/2024, procedo a elevar el presente dictamen técnico referente a la elaboración de las especificaciones técnicas tendientes a la realización de un procedimiento de contratación pública para la “ADQUISICIÓN DE EQUIPO FIREWALL PARA SEGURIDAD PERIMETRAL DE LA JUSTICIA ELECTORAL”, en los términos que paso a exponer a continuación:

#### II) MARCO NORMATIVO Y PARECER TÉCNICO

El Artículo 25°, primer apartado de la Ley N° 7021/2022 “DE SUMINISTRO Y CONTRATACIONES PÚBLICAS” dispone: “Para iniciar el procedimiento de contratación, la convocante deberá especificar al nivel más detallado posible los bienes, servicios, consultorías y obras públicas a adquirir con el fin de satisfacer sus necesidades...”.

El Artículo 40° del Decreto N° 9823/2023 “Por el cual se reglamenta la Ley N° 7021/2022 «DE SUMINISTRO Y CONTRATACIONES PÚBLICAS»” reza: “Las especificaciones técnicas que deban contener las bases de la contratación, se establecerán con la mayor amplitud de acuerdo con la naturaleza específica del contrato, con el objeto de que concurra el mayor número de oferentes...”.

El Artículo 40° de la Resolución DNCP N° 4401/23, modificado por el Art. 12 de la Resolución DNCP N° 453/24, el cual dispone: “La comunicación que realice la convocante a la DNCP a través del SICP, a los efectos de la verificación y la difusión de los procedimientos de contratación, además del pliego de bases y condiciones particular, deberá remitir mínimamente la siguiente documentación: a) Dictamen técnico en el cual se sustenten las especificaciones técnicas requeridas en el procedimiento de contratación, refrendado por el responsable del área requirente o del técnico que las recomendó...”.

Lo dispuesto por la Circular de la Dirección Nacional de Contrataciones Públicas N° 27/2024, que establece las Directrices o Modelo de Dictamen Técnico (Art.° 40 inc. a) Res. DNCP N° 4401 y Res DNCP N° 453 Art.° 12, en base a la cual se exponen los ítems y fundamentos conforme al siguiente detalle:

**UOC Convocante:** Justicia Electoral

**Unidad o área requirente:** Dirección de Tecnologías de la Información y Comunicación

**Funcionario o técnico responsable:** Lic. Fausto Von Streber

C.P. Angelo Calderini

Director

Unidad Operativa de Contratación

Fausto Von Streber  
Director de T.I.C.





## DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

\*\*\*\*\*

**Dependencia y cargo que desempeña:** Director de Tecnologías de la Información y Comunicación

- **Justificación técnica que respalda la objetividad, imparcialidad, regularidad y la razonabilidad o proporcionalidad de los requerimientos técnicos solicitados:**

Esta Dirección ha diseñado cuidadosamente las especificaciones técnicas y características del equipo de firewall por hardware en base a la creciente necesidad de fortalecer la seguridad cibernética de nuestra infraestructura informática, los cuales han demostrado que ofrecen una defensa sólida contra una amplia gama de amenazas, incluidos virus, malware avanzado entre otros ataques de día cero, los cuales son fundamentales para proteger nuestros sistemas asegurando la integridad contra amenazas externas e internas.

Considerando, la creciente sofisticación y complejidad de los ataques cibernéticos, se hace imprescindible fortalecer nuestra infraestructura de seguridad mediante la adquisición de dos (2) equipos de firewall por hardware, junto con sus sistemas de gestión correspondientes.

En términos técnicos adquirir estos equipos con sus características técnicas detalladas garantizan un alto rendimiento, seguridad y escalabilidad en la infraestructura de red de la institución. Ofrecen conectividad avanzada con puertos de alta velocidad, procesamiento eficiente con CPUs de múltiples núcleos y memoria ECC, y protección robusta contra amenazas cibernéticas, incluyendo ataques DDoS y tráfico malicioso. Además, cuentan con capacidades de virtualización de servicios de seguridad y control de tráfico, cumpliendo con estándares internacionales de calidad. Adquirir estos sistemas avanzados es una inversión estratégica que optimiza el rendimiento, mejora la seguridad, y ofrece escalabilidad para el crecimiento futuro de la institución.

Cabe destacar, que los equipos de firewall por hardware proporcionan una protección adicional, ya que permiten una detención más precisa y, por ende, una respuesta más rápida a posibles amenazas para nuestra red, lo que, junto con las herramientas de administración de firewall, permitirá gestionar y administrar de manera centralizada todas las políticas de seguridad, simplificando su configuración y supervisión.

En resumen, la adquisición de equipos de firewall con IPS y protección web avanzada es una medida esencial para fortalecer la seguridad de los equipos que componen la infraestructura tecnológica del Datacenter de la institución. Los equipos propuestos cumplen con todos los requisitos técnicos necesarios para ofrecer protección avanzada, alta disponibilidad y gestión centralizada, garantizando la protección frente a amenazas cibernéticas cada vez más complejas y sofisticadas.

- **Identificar y justificar de forma expresa si algún requerimiento podría limitar la participación de potenciales oferentes.**

No Aplica

C.P. Angelo Calderín  
Director  
Unidad Operativa de Contratación

Fausto Von Streber  
Director de T.I.C.

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN  
Y COMUNICACIÓN

\*\*\*\*\*

- Si en las bases licitatorias se indica una marca específica u otro derecho intelectual exclusivo, mencionar la justificación que respalda lo solicitado o que no existe otro modo de identificarlo. Se aclara que, en caso de incluirlos, los mismos tendrán carácter referencial.

No Aplica

III) ESPECIFICACIONES TÉCNICAS

Teniendo en cuenta la necesidad institucional cuya satisfacción se pretende, esta Dirección ha diseñado las especificaciones técnicas con las características específicas del bien requerido, que constituyen las más adecuadas teniendo en cuenta el relevamiento de datos realizado, el cual ayudó a determinar todos los detalles y requisitos que deben cumplir los equipos garantizando que aseguran las expectativas operativas y de protección a largo plazo.

Ítem N° 1 - EQUIPO FIREWALL PARA SEGURIDAD PERIMETRAL		
Características	Descripción Técnica	Mínimo Requerido
Tipo de instalación	En rack	Exigido
Tamaño máximo en Unidades de rack	1	Exigido
Interfaces	2 x 100 GE (QSFP28), 2 x 40 GE (QSFP+), 8 x 25 (ZSFP+), y 20 x 10 GE (SFP+)	Exigido
SFP+	Se deberá proveer con cada equipo 20 módulos SFP eléctricos como mínimo.	Exigido
CPU	2 CPUs, 16 cores por CPU, 2.0 GHz o superior como mínimo.	Exigido
Memoria	64 GB DDR4 ECC DIMM, 32 GB por CPU como mínimo.	Exigido
Memoria Flash	128 MB in total o superior	Exigido
Disco Duro	960 GB SATA 2.5" o superior.	Exigido
Puerto Consola	RJ45	Exigido
Máximo consumo en [W]	400 como máximo.	Exigido
MTBF [años]	35 o superior.	Exigido
Disponibilidad	0.99999	Exigido
Tipo de fuente de alimentación	Fuente de alimentación AC	Exigido
Numero de módulos de energía	2	Exigido
Fuente de alimentación redundante	1+1	Exigido

C.P. Angelo Calderini  
Director  
Unidad Operativa de Computación

Fausto Von Streber  
Director de T.I.C.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN  
Y COMUNICACIÓN

\*\*\*\*\*

<b>Voltaje de entrada [V]</b>	AC: 100 V - 240 V, 50 Hz/60 Hz	Exigido
<b>Rango de voltaje de entrada [V]</b>	AC: 90 V - 290 V, 45 Hz a 65 Hz	Exigido
<b>Numero de ventiladores</b>	4	Exigido
<b>Ajuste automático de velocidad de Ventiladores</b>	SI	Exigido
<b>Ventiladores redundantes</b>	3+1 o superior.	Exigido
<b>Ruido en condiciones normales [db(A)]</b>	≤75dB(A)	Exigido
<b>Temperatura de operación [°C(°F)]</b>	5°C - 40°C como mínimo.	Exigido
<b>Long-term operating relative humidity [RH]</b>	5% - 95% RH como máximo.	Exigido
<b>NGFW throughput</b>	40 Gbps o superior.	Exigido
<b>Threat protection throughput</b>	38 Gbps o superior.	Exigido
<b>Rendimiento del equipo en IPv4(1518/64/512 bytes)</b>	100/60/100 Gbps como mínimo.	Exigido
<b>Cantidad de conexiones concurrentes en IPv4</b>	50M o superior	Exigido
<b>URL category database scale (local)</b>	600K o superior	Exigido
<b>Numero de registros de listas negras estáticas</b>	20K o superior	Exigido
<b>Cantidad de políticas</b>	16K o superior	Exigido
<b>Cantidad de sistemas virtuales</b>	10 sistemas virtuales o más con soporte de expansión hasta 2K o superior	Exigido
<b>Cantidad de usuarios concurrentes en SSL VPN</b>	100 usuarios o más concurrentes con soporte de expansión hasta 20K	Exigido
<b>IPsec throughput</b>	60 Gbps o superior	Exigido
<b>Cantidad de túneles IPsec concurrentes</b>	Deberá soportar 80K o mas	Exigido

C. P. Angelo Calderini  
Director  
Unidad Operativa de Contratación

Fausto Von Streber  
Director de T.I.C.

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN  
Y COMUNICACIÓN

\*\*\*\*\*

<b>Cantidad de firmas IPS</b>	22K o superior	Exigido
<b>Capacidad de detección de aplicaciones</b>	60K o superior	Exigido
<b>URL category database scale (cloud)</b>	500M o superior	Exigido
<b>Cantidad de categorías URL</b>	45 categorías and 130 subcategorías o superior	Exigido
<b>Cantidad de VLANs en el sistema</b>	4K o superior.	Exigido
<b>Protección integrada</b>	Firewall, protección IPS, Antivirus, Anti DDoS, Filtro URL, VPN, gestión de Políticas	Exigido
<b>Control de Aplicaciones e Identificación</b>	Deberá identificar al menos 6000 aplicaciones y soportar control de acceso granular a las funciones de aplicaciones	Exigido
	Deberá combinar IPS e identificaciones de aplicaciones, filtro de datos, mejorando la exactitud	
<b>IPS &amp; protección Web</b>	Deberá obtener la última información sobre amenazas de manera a obtener la mejor precisión en la detección y defensa contra vulnerabilidades basadas en ataques.	Exigido
	Deberá soportar una cobertura de miles de CVE	
	Deberá detectar tráfico malicioso	
	Deberá detectar ataques de tráfico web como SQL inyección, cross-site scripting, botnets, control remoto, malwares y detección de ataques por fuerza bruta	
	Deberá soportar más de 20K firmas IPS y soporte por definición de firmas de usuario	
	Deberá detectar ataques por fuerza bruta basado en comportamiento de usuarios y definiciones de usuarios	
<b>Protección contra botnets</b>	Deberá contar con soporte para la detección de tráfico botnet usando funciones de IPS	Exigido
<b>Antivirus</b>	Deberá contar con inteligencia para detectar millones de variantes de virus mediante motor heurístico y soportar la detección en archivos comprimidos en 100 capas	Exigido
<b>Gestión de Ancho de banda</b>	Deberá soportar el manejo de ancho de banda basado en usuarios, IP, aplicaciones	Exigido
<b>Filtro URL</b>	Deberá poseer una base de datos de más 500 Millones de URLs y acelerar el acceso a categorías de sitios web específicos	Exigido
	Deberá soportar filtro DNS, en cada web accedida que es filtrada basada en Servidor de Nombre	
	Deberá soportar filtro URL anti-phishing	
<b>Seguridad de control industrial</b>	Deberá soportar el manejo y control de protocolos industriales como Modbus, DNP3, OPC, S7, CIP y Profinet	Exigido
	Deberá detectar y bloquear más de 100 sistemas de control como: SCADA/MES/PLC/HMI	
<b>Selección inteligente de link de subida</b>	Deberá realizar la selección de link de subida mediante múltiples algoritmos de balanceo	Exigido

C.P. Angelo Calderini  
Director  
Unidad Operativa de Contratación

Fausto Von Streber  
Director de T.I.C.



DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN  
Y COMUNICACIÓN

\*\*\*\*\*

<b>VPN</b>	Soporte para VPNs, Ipsec, SSL y GRE o superior.	Exigido
<b>Detección de tráfico encriptado SSL</b>	Deberá detectar y defender contra amenazas en tráfico encriptado SSL usando protección tipo IPS, AV filtro de datos y Filtros de URL	Exigido
<b>DDoS</b>	Deberá defender contra más de 10 tipos comunes de ataques DDoS incluyendo ataques SYN flood y UDP flood	Exigido
<b>Seguridad de Virtualización</b>	Deberá soportar de virtualización de múltiples tipos de servicios de seguridad incluyendo firewall, IPS, AV y VPN	Exigido
<b>Gestión de Políticas de Seguridad</b>	Deberá gestionar y controlar tráfico basado en VLAN Ids, seguridad por zonas, regiones, aplicaciones, categorías URL.	Exigido
	Deberá proveer escenarios predefinidos de defensas para facilitar el despliegue de políticas de seguridad	
<b>Routing</b>	Deberá soportar protocolos como OSPF, OSPFv3, BGP, RIP, IS-IS, BGP+, RIPng	Exigido
<b>IP multicast</b>	Soporte de protocolos Layer 3 como: MDSP, PIM y IGMP	Exigido
<b>Fiabilidad</b>	Deberá soportar modos HA, Activo/Activo y Pasivo/Standby	Exigido
<b>Servidor de Balanceo de Carga</b>	Deberá soportar equilibrio de cargas y persistencia de múltiples sesiones y métodos basados en direcciones IP de origen y cookies.	Exigido
	Deberá admitir la combinación de servicios y políticas de seguridad	
	Deberá admitir la verificación de estado basado en múltiples protocolos como TCP, RADIUS, DNS y HTTP	
<b>Cumplimientos y regulaciones</b>	IEC 60825, CDRH 21 o similar, FCC o similar, WEEE, REACH, VCCI class A o similar	Exigido
<b>Todas las funcionalidades solicitadas en estas EETT</b>	Deberán estar activas y utilizables por un periodo mínimamente de 12 meses al momento de entrega del equipo.	Exigido
<b>Autorización</b>	Autorización del fabricante, representante o distribuidor del bien ofertado en caso de que la empresa oferente no haya fabricado o elaborado el producto ofertado.	Exigido
<b>Garantía de fábrica</b>	Garantía de al menos 3 años de fábrica de los equipos ofertados a partir de la recepción por parte de la convocante. La carta de garantía deberá estar firmada por el fabricante o distribuidor autorizado en el Paraguay de la marca de los equipos ofertados. La garantía permite el reemplazo de partes sin costo para la convocante por problemas de fabricación o diseño de los equipos ofertados.	Exigido

Por lo expuesto, la Dirección de Tecnologías de la Información y Comunicación considera que las Especificaciones Técnicas del bien solicitado se encuentra debidamente sustentada técnicamente, conforme a la necesidad institucional, atendiendo a que la misma fueron diseñada a los efectos de asegurar las mejores condiciones de contratación en cuanto a oportunidad, calidad y costo se refiere.



Director  
Unidad Operativa de Contratación

Es mi dictamen.-

Lic. Fausto Von Streber  
Director de Tecnologías de la Información y Comunicación

