Asunción, 22 de noviembre de 2012

LICITACION PUBLICA NACIONAL N° 21/2012 – CONSTRUCCION DE OBRA PARA CENTRO DE DATOS – ID N° 244.784

ADENDA N° 1

El Ministerio de Justicia y Trabajo de conformidad al Art. 22 de la Ley Nº 2051 inciso "b", el Art. 40 del Decreto Nº 21.909, que reglamenta la citada Ley y en uso de sus atribuciones, emite la siguiente Adenda, a fin de realizar las modificaciones en la Planilla de Precios y planillas de especificaciones técnicas 15, 16, 17, 29, 30 y 31.

MODIFICACIONES:

Sección IV. Formularios de la Oferta

Lista de Cantidades y sus Precios

1	2	4	5	6	7	8
Ítem	**Código de Catálogo**	**Descripción**	**Unidad de Medida**	**Cant.**	**Precio unitario** (IVA incluido si correspondiese)	**Precio Total** (IVA incluido si correspondiese)
1- CONSTRUCCIÓN DE UN CENTRO DE DATOS PARA EL REGISTRO CIVIL						
A - OBRAS CIVILES						
1	72101607-007	Pared de ladrillos comunes 0.30	*m 2*	140		
2	72101607-006	Revoque de paredes con aislación hidrófuga	m 2	280		
3	72102508-001	Carpeta de nivelación	m 2	60		
4	72102402-001	Pintura de Pared	m 2	140		
5	72131601-007	Techo de estructura metalica con perfles doble "C"de 12 cm espesor 2mm y chapa acanalada AT105. Prever bavetas de borde	m 2	60		
6	72102201-003	Estructura portante para las cargas viva y muerta	Unidad	1		
7	72102602-005	Puerta Metalica para acceso al ambiente de seguridad compuestas por capas de acero 120 mm de grosor minimo	Unidad	1		
8	72102201-003	Sala Cofre, hermetica contra gases y Agua, proteccion refractaria, estabilidad termica segun especificacion tecnica	Unidad	1		
9	72102701-999	Piso Técnico: de 50 cm. De altura. Incluye Piso elevado estándar y piso elevado de placas perforadas	m 2	60		
10	72102305-002	Instalacion de sistema de Aire Acondicionado	Unidad	2		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

B- INSTALACIONES ELECTRICAS						
11	72102201-003	Instalacion de Tablero Electrico Principal	Unidad	1		
12	72102201-004	Instalacion de tablero de transferencia automotica de generador	Unidad	1		
13	72102201-003	Instalacion de tablero electrico en el centro de datos	Unidad	1		
14	72102201-003	Alimentación eléctrica tipo industrial para Racks	Unidad	12		
15	72102201-003	Cableado electrico para equipos e iluminacion segun especificaciones tecnicas	Global	1		
16	72102201-003	Instalacion de sistema de apagado de emergencia (EPO)	Unidad	1		
17	72102201-003	Sistema de puesta a tierra	Unidad	1		
18	72102201-004	Instalacion de Grupo Electrogeno	Unidad	1		
19	39121004-003	Instalacion de UPS	Unidad	2		
C- INSTALACIONES VARIAS						
20	92121702-001	Sistema contra incendio que incluye Panel Central convencional con agente de descarga, Sensor de Humo y Calor, Teclado anunciador remoto, Pulsador Manual de incendio con botón de parada de descarga, Alarma audiovisual con modulo direccionable, Unidad de Extinción con gas NAF S 125 o NAFS II y todos los materiales para instalacion segun eett	Global	1		
21	46171610-002	Cámara IP Tipo 1 Mini Domo Para Interiores	Unidad	2		
22	46171610-002	Cámara IP Tipo 2 Mini Domo Anti Vandálica	Unidad	2		
23	46171621-001	Grabador de Video y Control de Acceso	Unidad	1		
24	26121607-001	Instalacion de Cableado Estructurado dentro del centro de datos	Unidad	1		
25	26121607-001	Instalacion del backbone de fibra opotica externo del Registro Civil	Unidad	1		
26	26121607-001	Instalacion del Backbone de fibra optica interno del Registro Civil	Unidad	1		
27	72102203-002	Installacion del sitema de monitoreo remoto	Unidad	1		
28	26111501-011	Instalacion de Racks en la sala cofre	Unidad	12		
29	26111501-011	Instalacion de Rack	Unidad	1		
30	43211508-001	Computadoras de Escritorio	Unidad	2		
31	56101504-002	Sillas Giratorias	Unidad	2		
32	56101703-002	Escritorio	Unidad	2		
33	26111501-020	Switch de core	Unidad	1		
34	43222609-001	Router/Firewall de core	Unidad	1		
35	26111501-006	Switch de distribución	Unidad	5		
2- CONSTRUCCIÓN DE UN CENTRO DE DATOS PARA EL MINISTERIO DE JUSTICIA Y TRABAJO						
A - OBRAS CIVILES						
36	72103003-001	Preparacion de infraestructura existente	Global	1		
37	72102602-005	Puerta Metalica para acceso al centro de datos	Unidad	1		
38	72102201-003	Ambiente de seguridad para equipos criticos	Unidad	1		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

39	72102701-999	Piso Técnico: de 50 cm. De altura. Incluye Piso elevado estándar y piso elevado de placas perforadas	m 2	120		
40	72102305-002	Instalacion de sistema de Aire Acondicionado	Unidad	2		
B- INSTALACIONES ELECTRICAS						
41	72102402-001	Pintura de Pared	m 2	120		
42	72102201-003	Instalacion de Tablero Electrico Principal	Unidad	1		
43	72102201-003	Instalacion de tablero electrico en el centro de datos	Unidad	1		
44	72102201-003	Alimentación eléctrica tipo industrial para Racks	Unidad	4		
45	72102201-003	Cableado electrico para equipos e iluminacion segun especificaciones tecnicas	Global	1		
46	72102201-003	Instalacion de sistema de apagado de emergencia (EPO)	Unidad	1		
47	72102201-003	Sistema de puesta a tierra	Unidad	1		
48	39121004-003	Instalacion de UPS	Unidad	2		
C- INSTALACIONES VARIAS						
49	92121702-001	Sistema contra incendio que incluye Panel Central convencional con agente de descarga, Sensor de Humo y Calor, Teclado anunciador remoto, Pulsador Manual de incendio con botón de parada de descarga, Alarma audiovisual con modulo direccionable, Unidad de Extinción con gas NAF S 125 o NAFS II y todos los materiales para instalacion segun eett	Global	1		
50	46171610-002	Cámara IP Tipo 1 Mini Domo Para Interiores	Unidad	2		
51	46171610-002	Cámara IP Tipo 2 Mini Domo Anti Vandálica	Unidad	2		
52	46171621-001	Grabador de Video y Control de Acceso	Unidad	1		
53	72102203-002	Instalacion de Cableado Estructurado dentro del centro de datos	Unidad	1		
54	26121607-001	Instalacion del Backbone de fibra optica interno del MJT	Unidad	1		
55	72102203-002	Installacion del sitema de monitoreo remoto	Unidad	1		
56	26111501-011	Instalacion de Racks	Unidad	4		
57	26111501-011	Instalacion de Rack	Unidad	1		
58	43211508-001	Computadoras de Escritorio	Unidad	2		
59	56101504-002	Sillas Giratorias	Unidad	10		
60	56101703-002	Escritorio	Unidad	10		
61	26111501-020	Switch de core	Unidad	1		
62	43222609-001	Router/Firewall de core	Unidad	1		
63	26111501-006	Switch	Unidad	5		
64	26111501-006	Switch controlador	Unidad	1		
65	43221718-002	Equipo Access Point	Unidad	5		
66	72102203-002	Instalacion de puntos de Cableado Estructurado de Datos dentro del edificio del MJT	Unidad	200		
TOTAL						-

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

PARTE 2 – Obras Requeridas

Sección V. Alcance de las Obras

4. LISTA ESTIMADA DE CANTIDADES

1	2	3	4	5
Ítem	**Código de Catálogo**	**Descripción**	**Unidad de Medida**	**Cant.**
1 - CONSTRUCCIÓN DE UN CENTRO DE DATOS PARA EL REGISTRO CIVIL				
A - OBRAS CIVILES				
1	72101607-007	Pared de ladrillos comunes 0.30	*m 2*	140
2	72101607-006	Revoque de paredes con aislación hidrófuga	m 2	280
3	72102508-001	Carpeta de nivelación	m 2	60
4	72102402-001	Pintura de Pared	m 2	140
5	72131601-007	Techo de estructura metalica con perfles doble "C"de 12 cm espesor 2mm y chapa acanalada AT105. Prever bavetas de borde	m 2	60
6	72102201-003	Estructura portante para las cargas viva y muerta	Unidad	1
7	72102602-005	Puerta Metalica para acceso al ambiente de seguridad compuestas por capas de acero 120 mm de grosor minimo	Unidad	1
8	72102201-003	Sala Cofre, hermetica contra gases y Agua, proteccion refractaria, estabilidad termica segun especificacion tecnica	Unidad	1
9	72102701-999	Piso Técnico: de 50 cm. De altura. Incluye Piso elevado estándar y piso elevado de placas perforadas	m 2	60
10	72102305-002	Instalacion de sistema de Aire Acondicionado	Unidad	2
B- INSTALACIONES ELECTRICAS				
11	72102201-003	Instalacion de Tablero Electrico Principal	Unidad	1
12	72102201-004	Instalacion de tablero de transferencia automotica de generador	Unidad	1
13	72102201-003	Instalacion de tablero electrico en el centro de datos	Unidad	1
14	72102201-003	Alimentación eléctrica tipo industrial para Racks	Unidad	12
15	72102201-003	Cableado electrico para equipos e iluminacion segun especificaciones tecnicas	Global	1
16	72102201-003	Instalacion de sistema de apagado de emergencia (EPO)	Unidad	1
17	72102201-003	Sistema de puesta a tierra	Unidad	1
18	72102201-004	Instalacion de Grupo Electrogeno	Unidad	1
19	39121004-003	Instalacion de UPS	Unidad	2

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

C- INSTALACIONES VARIAS				
20	92121702-001	Sistema contra incendio que incluye Panel Central convencional con agente de descarga, Sensor de Humo y Calor, Teclado anunciador remoto, Pulsador Manual de incendio con botón de parada de descarga, Alarma audiovisual con modulo direccionable, Unidad de Extinción con gas NAF S 125 o NAFS II y todos los materiales para instalacion segun eett	Global	1
21	46171610-002	Cámara IP Tipo 1 Mini Domo Para Interiores	Unidad	2
22	46171610-002	Cámara IP Tipo 2 Mini Domo Anti Vandálica	Unidad	2
23	46171621-001	Grabador de Video y Control de Acceso	Unidad	1
24	26121607-001	Instalacion de Cableado Estructurado dentro del centro de datos	Unidad	1
25	26121607-001	Instalacion del backbone de fibra opotica externo del Registro Civil	Unidad	1
26	26121607-001	Instalacion del Backbone de fibra optica interno del Registro Civil	Unidad	1
27	72102203-002	Installacion del sitema de monitoreo remoto	Unidad	1
28	26111501-011	Instalacion de Racks en la sala cofre	Unidad	12
29	26111501-011	Instalacion de Rack	Unidad	1
30	43211508-001	Computadoras de Escritorio	Unidad	2
31	56101504-002	Sillas Giratorias	Unidad	2
32	56101703-002	Escritorio	Unidad	2
33	26111501-020	Switch de core	Unidad	1
34	43222609-001	Router/Firewall de core	Unidad	1
35	26111501-006	Switch de distribución	Unidad	5
2- CONSTRUCCIÓN DE UN CENTRO DE DATOS PARA EL MINISTERIO DE JUSTICIA Y TRABAJO				
A - OBRAS CIVILES				
36	72103003-001	Preparacion de infraestructura existente	Global	1
37	72102602-005	Puerta Metalica para acceso al centro de datos	Unidad	1
38	72102201-003	Ambiente de seguridad para equipos criticos	Unidad	1
39	72102701-999	Piso Técnico: de 50 cm. De altura. Incluye Piso elevado estándar y piso elevado de placas perforadas	m 2	120
40	72102305-002	Instalacion de sistema de Aire Acondicionado	Unidad	2
B- INSTALACIONES ELECTRICAS				
41	72102402-001	Pintura de Pared	m 2	120
42	72102201-003	Instalacion de Tablero Electrico Principal	Unidad	1
43	72102201-003	Instalacion de tablero electrico en el centro de datos	Unidad	1
44	72102201-003	Alimentación eléctrica tipo industrial para Racks	Unidad	4
45	72102201-003	Cableado electrico para equipos e iluminacion segun especificaciones tecnicas	Global	1
46	72102201-003	Instalacion de sistema de apagado de emergencia (EPO)	Unidad	1
47	72102201-003	Sistema de puesta a tierra	Unidad	1

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

48	39121004-003	Instalacion de UPS	Unidad	2
C- INSTALACIONES VARIAS				
49	92121702-001	Sistema contra incendio que incluye Panel Central convencional con agente de descarga, Sensor de Humo y Calor, Teclado anunciador remoto, Pulsador Manual de incendio con botón de parada de descarga, Alarma audiovisual con modulo direccionable, Unidad de Extinción con gas NAF S 125 o NAFS II y todos los materiales para instalacion segun eett	Global	1
50	46171610-002	Cámara IP Tipo 1 Mini Domo Para Interiores	Unidad	2
51	46171610-002	Cámara IP Tipo 2 Mini Domo Anti Vandálica	Unidad	2
52	46171621-001	Grabador de Video y Control de Acceso	Unidad	1
53	72102203-002	Instalacion de Cableado Estructurado dentro del centro de datos	Unidad	1
54	26121607-001	Instalacion del Backbone de fibra optica interno del MJT	Unidad	1
55	72102203-002	Installacion del sitema de monitoreo remoto	Unidad	1
56	26111501-011	Instalacion de Racks	Unidad	4
57	26111501-011	Instalacion de Rack	Unidad	1
58	43211508-001	Computadoras de Escritorio	Unidad	2
59	56101504-002	Sillas Giratorias	Unidad	10
60	56101703-002	Escritorio	Unidad	10
61	26111501-020	Switch de core	Unidad	1
62	43222609-001	Router/Firewall de core	Unidad	1
63	26111501-006	Switch	Unidad	5
64	26111501-006	Switch controlador	Unidad	1
65	43221718-002	Equipo Access Point	Unidad	5
66	72102203-002	Instalacion de puntos de Cableado Estructurado de Datos dentro del edificio del MJT	Unidad	200

6. ESPECIFICACIONES TECNICAS

2. ESPECIFICACIONES TÉCNICAS PARA LA PLANILLA DEL REGISTRO CIVIL

2.12. Equipos Activos

Se solicitan en este proyecto un Switch de Core, un Router/Firewall de Core y equipos de distribución LAN.

2.12.1. Núcleo

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Planilla N° 15 - Especificaciones técnicas			
Equipo Switch de core			
Equipo Switch de core	**Características**	**El bien ofertado cumple con las especificaciones requeridas (si/no)**	**Especificaciones técnicas ofertadas**
Cantidad	(01) uno		
Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Descripción	Switch de core		
Características Principales			
Fuente de Poder y redundancia	Dos, en modalidad redundante VAC 220 VAC @ 50 Hz.		
	Deberá soportar el intercambio de estas fuentes redundantes de poder en caliente, sin necesidad de bajar el equipo.		
	Deberá contar con 2 fuentes de poder trabajando en redundancia 1+1		
	Deberá contar con redundancia de cooling en la modalidad 3+1		
Interfaces	El equipo deberá poseer al menos 40 interfaces fijas SFP/SFP+ que soporten 1GbE/10GbE respectivamente con soporte de módulos ópticos y/o eléctricos intercambiables entre cualquiera de ellos.		
	El equipo deberá tener la capacidad de soportar hasta 64 interfaces de 10GbE SFP+ a través de módulos de		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	expansión		
	El equipo deberá tener la capacidad de soportar al menos 6 interfaces de 40GbE a través de módulos QSFP+		
Soporte de protocolos de enlaces de Fibra Óptica y Cobre	1000Base-T		
	1000Base-SX		
	1000Base-LX		
	1000Base-LH40		
	1000Base-LH70		
	10GbE-SR		
	10GbE-LR		
	10GbE-ER		
	10GbE-LRM		
	Todos los tipos de interfaces deben poder operar en modalidad Full Duplex.		
Transceivers solicitados	2 (uno) SFP+ 10 Gb Multimodo		
	2 (uno) SFP+ 10 Gb Monomodo		
	14 (Catorce) SFP Óptico Multimodo de 1 Gb		
	16 (Diez y Seis) SFP 1000BT (elecetrico)		
Del Sistema	Para la solución propuesta debe incluirse todo lo necesario para el correcto funcionamiento de todo el conjunto, es decir, accesorios y conexiones incluyendo a los equipos e instalaciones actuales.		
Switch Multilayer			
Alta Disponibilidad	El equipo básico debe disponer de un ancho de banda efectivo no menor a 1.2 Tbps provisto por un switching fabric no bloqueante.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Deberá tener capacidad de Alta disponibilidad en enlaces para los equipos conectados a estos switches a nivel de capa 2 a través de conexión de al menos 2 de estos switches de core brindando redundancia de enlaces del tipo Activo/Activo. No se aceptarán aplicaciones de Spanning Tree para este requerimiento. Ninguna performance se deberá ver afectada con la caída de uno de los dos equipos trabajando en una de estas tecnologías citadas		
	El oferente deberá detallar y documentar mediante especificaciones técnicas originales del fabricante el funcionamiento de la Alta Disponibilidad ó High Availability del equipo.		
Performance	900 Mpps de 64 bytes (700 Millones de paquetes por segundo de 64 bytes cada uno).		
	La latencia máxima de los paquetes de 64 bytes deberá ser de: 7 µs en Capas 2 y 3 sobre interfaces 10 Gbe.		
	Capacidad de memoria SDRAM		
	Capacidad de memoria FLASH		
	Tamaño de tabla de Mac Address en L2		
	Tamaño de tabla de IPv4 en L3		
	Tamaño de tabla de IPv6 en L3		
	Tamaño de tabla para grupos MCAST		
	Tamaño de tablas para ACL		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Tamaño de tablas para Link Aggregation: 32 grupos trunks, 2 a 8 puertos por grupos de trunk		
Características Adicionales del Equipo			
Normas ó recomendaciones internacionales	IEEE 802.1d		
	IEEE 802.1p		
	IEEE 802.1q VLAN tagging (La cantidad de VLANs IDs no podrá ser inferior a 4.000).		
	IEEE 802.1s Per-VLAN Group Spanning Tree Protocol.		
	IEEE 802.1w RSTP.		
	IEEE 802.1x IBNS-Identity Based Networking Services.		
	IEEE 802.3ad Link aggregation control protocol.		
	IEEE 802.3ab 1000BASE-T.		
	IEEE 802.3ae 10 Gigabit Ethernet.		
	IEEE 802.3z 1000BaseSX/ 1000BaseLX/100BaseLH.		
	RFC 768 User Datagram Protocol (UDP).		
	RFC 783 Trivial File Transfer Protocol (TFTP).		
	RFC 791 IP.		
	RFC 792 Internet Control Message Protocol (ICMP).		
	RFC 793 TCP.		
	RFC 826 Address Resolution Protocol (ARP).		
	RFC 854 Telnet.		
	RFC 894 IP over Ethernet.		
	RFC 903 Reverse Address Resolution Protocol (RARP).		
	RFC 906 TFTP Bootstrap.		
	RFC 951, 1542 BOOTP, BOOTP extensions.		
	RFC 1027 Proxy ARP.		
	RFC 1122 Host requirements.		
	RFC 1519 Classless		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	interdomain routing (CIDR).		
	RFC 1886 Domain Name System (DNS)		
	RFC 1812 IPv4.		
	RFC 2131 BOOTP/DHCP.		
	RFC 2338 VRRP.		
	RFC 1112 Internet Group Management Protocol (IGMP).		
	RFC 2236 IGMP v1, v2, v3 snooping.		
	RFC 1583 OSPFv2.		
	RFC 1587 OSPF NSSA.		
	RFC 1745		
	RFC 1765 OSPF database overflow.		
	RFC 1850 OSPFv2 Management Information Base (MIB), traps.		
	RFC 1997 BGP Communities and attributes.		
	RFC 2154 OSPF digital signatures, MD5.		
	RFC 2370 OSPF opaque link-state advertisement (LSA) option.		
	RFC 1058 RIPv1.		
	RFC 2453 RIPv2.		
	RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6, and Open Systems Interconnection (OSI)		
	RFC 854 Telnet.		
	RFC 951 BOOTP.		
	RFC 1213 SNMP MIB II.		
	RFC 1724 RIPv2 MIB.		
	RFC 3418 SNMPv2c.		
	RFC 1492 TACACS+.		
	RFC 2865 RADIUS authentication.		
	SPAN.		
	Control y bloqueo de Media Access Control (MAC) address para seguridad.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	RADIUS accounting		
	Autenticación vía RADIUS por cada comando.		
	Limite de ancho de banda real por cualquier criterio de Capas 2.		
	Se hace especial hincapié en el soporte de QoS, el equipo debe soportar el marcado, re-marcado, priorización y tratamiento de paquetes en distintas calidades de servicio por cualquier criterio de Capas 1, 2, 3 y 4 sin que ello afecte la performance del equipo (Ver especificaciones de performance y su impacto ante la aplicación de las distintas políticas de QoS).		
	El equipo debe soportar el manejo de frames ó tramas Ethernet de tamaño mayor al Standard específicamente debe soportar Jumbo Frames de 9.216 bytes y Giant babies de 1600 bytes.		
	RFC 3768 Virtual Router Redundancy Protocol		
Normas o reglamentaciones internacionales Adicionales	RFC 1771 BGP4.		
	RFC 1965 BGP4 autonomous system confederations.		
	RFC 2796 BGP4 route reflection.		
	RFC 1997 Communities attribute.		
	RFC 2385 Transmission Control Protocol (TCP) Message Digest Algorithm 5 (MD5) authentication for BGP.		
	RFC 2439 Route flap dampening.		
	RFC 2796 Route reflection.		
	RFC 2842 Capabilities		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	advertisement.		
	RFC 2068 HTTP.		
	DHCP Server.		
	DHCP Server por VLAN		
	Los equipos deben disponer de interfaces de salida que operen en 2da. Ventana (~1310nm) y 3ra. Ventana (~1550nm) compatible con la norma G.652.		
	El equipo soportará la facilidad de IGMP "snooping".		
	El equipo debe soportar la posibilidad de la sincronización horaria de los diferentes nodos de red.		
	El equipo debe disponer de interfaces virtuales con las mismas funcionalidades de las interfaces físicas.		
	El equipo debe permitir establecer direcciones IP secundarias (adicionales) en sus interfaces.		
Tráfico y Calidad de Servicio	Soporte de sumarización de rutas y redes (CIDR).		
	Prioridad de colas: 8 colas por puerto basado en hardware		
	Priorización de tráfico: QoS basado en tráfico		
	Gestión de control de ancho de banda basado en flujo		
	gestión de colas con configuración de agendamiento de algoritmos		
	RED, WRED		
	Arquitectura DiffServ		
Administración	El equipo debe disponer de un puerto serial RS-232 para conectar la gestión local, en caso de ser propietario, deben contar con su correspondiente adaptador.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El equipo en su gestión local debe disponer un mínimo de 3 niveles de acceso de usuario con diferentes atributos de modificación.		
	El nivel más alto de gestión local debe poder definir la lista de usuarios con su clave de acceso (password de al menos 8 caracteres) y sus atributos asociados.		
	Las claves de acceso (password) que contenga el equipo deben estar encriptados y no serán visibles por ningún comando de visualización.		
	Dentro de las prestaciones de la gestión local se debe disponer de un comando de visualización de eventos (log) encolados por aparición (tipo FIFO).		
	El equipamiento debe poder ser administrado/gestionado por los protocolos SNMPv1, SNMPv2, SNMPv3, RMON.		
	Deberá ser accesible local y remotamente con las mismas facilidades en ambas modalidades mediante protocolos seguros de comunicación, como mínimo SSH.		
	Deberá poder ser 100% administrable remotamente, pudiendo efectuar actualizaciones remotas de su sistema operativo sin que se interrumpa la comunicación con la estación de gerenciamiento y management.		
Instalación	Todos los trabajos serán ejecutados de acuerdo a las reglas del arte y presentarán, una vez terminados, un		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	aspecto prolijo y mecánicamente resistente.		
	Proveer los accesorios necesarios para la realización de las tareas: cintas, tornillos, arandelas, etc.		
	Además de cumplir con lo establecido en la presente documentación, las instalaciones deberán ser ejecutadas en un todo de acuerdo con los reglamentos para instalaciones de los estándares internacionales.		
	Se deberá prever las perforaciones y el anclaje necesario del rack dentro de la estructura de piso técnico del Data Center actual.		
Demostración	Se reserva el derecho de solicitar una demostración del equipo ofertado si fuese necesario.		
MTBF	140.000 horas		
Fabricación	Todos los equipos deben ser nuevos, de fabricación reciente, encontrarse en comercialización.		
Certificación de calidad	Certificación ISO 9000 para todos los materiales utilizados.		
Garantía	Soporte de atención, repuestos, Mano de Obra y mantenimiento correctivo a cargo del Oferente		
Autorización del Fabricante para presentar oferta y certificación técnica.	Autorización escrita para presentar oferta. Técnicos certificados por fabrica (presentar documentación)		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

2.12.2. Firewall de Core

Planilla N° 16 - Especificaciones técnicas			
Equipo Router/Firewall de core			
Equipo Router/Firewall de core	**Características**	**El bien ofertado cumple con las especificaciones requeridas (si/no)**	**Especificaciones técnicas ofertadas**
Cantidad	(01) uno		
Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Descripción	Router/Firewall de core		
Características Principales			
Definición:	Sistema de Seguridad informática que sea del tipo Administración Unificada de Amenazas, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que abajo se detallan, pudiendo ser todas ellas en una sola caja o en cajas diferentes.		
Funcionalidades y características del sistema			
Características de Desempeño:	Throughput Firewall @64/512/1500 Bytes: 20 Gbps		
	Throughput IPsec VPN: 8 Gbps		
	Throughput IPS: 6 Gbps		
	Throughput AV: 2.1 Gbps		
	Sesiones concurrentes: 7 Mil		
	Nuevas sesiones por segundo: 190.000		
Características de Hardware:	Interfaces GigaEthernet 10/100/1000: 12		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Interfaces 10GigE: 2 SFP+		
	Almacenamiento Tamaño (GB): 128 GB		
Características del dispositivo:	El dispositivo debe ser una appliance de propósito específico		
	Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.		
	Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).		
	Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).		
	El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red.		
	En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Características del Sistema operativo incluido:	Sistema operativo pre-endurecido específico para seguridad que sea compatible con el appliance. Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows		
	El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.		
Firewall:	Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs		
	Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.		
	Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando		
	Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.		
	Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación		
	Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.		
	Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo		
	Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)		
	Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.		
	Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.		
	Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.		
	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)		
	La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas		
	En la solución de balanceo de carga entre servidores, debe soportarse persitencia de sesión al menos mediante HTTP Cookie o SSL Session ID		
	En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.		
Conectividad y sistema de ruteo:	Se debe considerar al menos el tener una interface/puerto DMZ y 2 puertos para enlaces WAN.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP		
	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs		
	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas		
	Soporte a políticas de ruteo (policy routing)		
	El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace		
	Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS		
	Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+		
	La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.		
	Soporte de ECMP (Equal Cost Multi-Path)		
	Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.		
	Soporte a ruteo de multicast		
	La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.		
VPN Ipsec/L2TP/PPTP:	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)		
	Soporte para IKEv2 y IKE Configuration Method		
	Debe soportar la configuración de túneles L2TP		
	Debe soportar la configuración de túneles PPTP		
	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.		
	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits		
	Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.		
	Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.		
	Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.		
	La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)		
	En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.		
	Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.		
	Capacidad minima de tuneles - GW to GW (10.000 tunel IPsec) - GW to client (50.000 tunel IPsec)		
VPN SSL:	Capacidad de realizar SSL VPNs.		
	Soporte a certificados PKI X.509 para construcción de VPNs SSL.		
	Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.		
	Soporte de renovación de contraseñas para LDAP y		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	RADIUS.		
	Soporte a asignación de aplicaciones permitidas por grupo de usuarios		
	Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.		
	Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.		
	Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)		
	La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS		
	Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL		
	Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.		
	Los portales personalizados deberán soportar al menos la definición de:		
	Widgets a mostrar		
	Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC		
	Esquema de colores		
	Soporte para Escritorio Virtual		
	Política de verificación de la estación de trabajo.		
	La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.		
	En la configuración del Escritorio Virtual podrá definirse como mínimo:		
	La posibilidad de que el usuario cambie entre escritorio virtual y real.		
	La posibilidad de restringir el acceso a la memoria (clipboard) del escritorio virtual desde el escritorio real.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	La posibilidad de utilizar medios removibles desde el escritorio virtual		
	La posibilidad de acceder a recursos compartidos desde el escritorio virtual		
	La posibilidad de imprimir desde el escritorio virtual.		
	La posibilidad de definir y restringir las aplicaciones que podrán ser ejecutadas en el escritorio virtual.		
Traffic Shapping / QoS:	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall		
	Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión		
	Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.		
	Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo		
	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo		
	Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Capacidad de integrarse con Servidores de Autenticación RADIUS.		
	Capacidad nativa de integrarse con directorios LDAP		
	Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"		
Autenticación y Certificación Digital:	Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.		
	Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.		
	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)		
	Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.		
	Soporte de verificación de validación de certificados digitales mediante el		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	protocolo OSCP (Online Simple Enrrollment Protocol)		
	La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.		
	Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.		
	Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:		
	Longitud mínima permitida		
	Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.		
	Expiración de contraseña.		
	Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP		
Antivirus:	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.		
	Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.		
	El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.		
	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.		
	El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List)		
	El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP		
	El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.		
	El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.		
	El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.		
	El antivirus deberá ser capaz de filtrar archivos por extensión		
	El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)		
Antispam:	La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.		
	La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)		
	La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	mecanismos para detección de SPAM		
	En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.		
Filtraje de URLs (URL Filtering):	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.		
	Debe poder categorizar contenido Web requerido mediante IPv6.		
	Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.		
	Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida		
	Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.		
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).		
	La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.		
	Será posible exceptuar la inspección de HTTPS por categoría.		
IPS:	El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de linea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror		
	El detector y preventor de intrusos podrá implementarse en linea y fuera de linea en forma simultánea para distintos segmentos.		
	Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6		
	Capacidad de detección de más de 4000 ataques.		
	Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El Detector y preventor de intrusos deberá de estar orientado para la protección de redes.		
	El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.		
	El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).		
	Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.		
	Tecnología de detección tipo Stateful basada en Firmas (signatures).		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Actualización automática de firmas para el detector de intrusos		
	El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.		
	Mecanismos de detección de ataques: § Reconocimiento de patrones, Análisis de protocolos, § Detección de anomalías § Detección de ataques de RPC (Remote procedure call) § Protección contra ataques de Windows o NetBios § Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol) § Protección contra ataques DNS (Domain Name System) § Protección contra ataques a FTP, SSH , Telnet y rlogin § Protección contra ataques de ICMP (Internet Control Message Protocol).		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Métodos de notificación: § Alarmas mostradas en la consola de administración del appliance. § Alertas vía correo electrónico. § Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque.Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. § La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto.		
	Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP		
Prevención de Fuga de Información (DLP):	La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.		
	Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.		
	Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento,		
	En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.		
	La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.		
	La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.		
Control de Aplicaciones:	Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.		
	Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.		
	El listado de aplicaciones debe actualizarse periódicamente.		
	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.		
	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.		
	Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.		
	Preferentemente deben soportar mayor granularidad en las acciones.		
Inspección de Contenido SSL:	La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.		
	La inspección deberá realizarse mediante la técnica conocida como		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Hombre en el Medio (MITM – Man In The Middle).		
	La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.		
	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.		
Cache Web:	La solución debe soportar actuar como un cache web, entendiéndose como la capacidad de almacenar contenido estátic que será servido localmente en posteriores requerimientos.		
	Debe poder definirse el tamaño del almacenamiento dedicado para la función de web cache.		
	Debe poder definirse el máximo tiempo en el que un objeto permanecerá en el caché (TTL).		
	El web cache debe configurarse mediante reglas que definirán el contenido que debe ser almacenado al menos con los siguientes parámetros: Dirección IP o grupo de direcciones IP de origen,		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	dirección IP o grupo de direcciones IP de destino, rango de puertos de destino.		
	El Cache Web podrá configurarse en forma transparente. En este modo, no es necesario que el navegador del usuario tenga configurado un Proxy.		
	El Caché Web podrá configurarse como un Proxy HTTP explícito en la red. Esto significa que los navegadores podrán configurar el dispositivo FortiGate como Proxy para la navegación.		
	Soporte del protocolo WCCPv2. Este protocolo debe soportarse en modo cliente como en modo servidor. En modo servidor, el dispositivo será capaz de redireccionar el tráfico Web hacia uno o más servidores de Caché Web en modo transparente para el usuario final. En modo cliente, el dispositivo podrá comportase como un Web Caché al cual se le redireccionará tráfico por un servidor de WCCPv2		
	WCCPv2 deberá soportarse tanto con GRE como Layer 2 forwarding.		
	La solución debe soportar la capacidad de aplicar el Caché Web a tráfico		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	encriptado con SSL (HTTPS).		
	Cuando la solución se encuentre configurada como un Proxy explícito, éste debe poder habilitarse de forma diferenciada por interfaz de red.		
	En Proxy explícito la solución debe soportar los siguientes protocolos: HTTP, HTTPS, FTP y SOCKS		
	En Proxy explícito debe poder configurarse de forma independiente los puertos en los que estarán activos los siguientes protocolos: HTTP, HTTPS, FTP y SOCKS.		
	En Proxy explícito la solución debe soportar la configuración automática de los navegadores mediante PAC File (Proxy Auto-Configuration File)		
Optimización de WAN	La solución deberá soportar la capacidad de disminuir el tráfico transmitido por un determinado enlace mediante diferentes técnicas.		
	El Optimización de WAN debe configurarse mediante reglas que definirán el tráfico a optimizar al menos con los siguientes parámetros: Dirección IP o grupo de direcciones IP de origen, dirección IP o grupo de direcciones IP de destino, rango de puertos de destino.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Deberán utilizarse al menos las siguientes técnicas para Optimización WAN: Compresión, Byte Caching, Object Caching		
	En caso de requerirse un dispositivo en ambos extremos del enlace de comunicaciones, debe ser posible autenticar las partes antes de establecer la optimización		
	La solución debe tener la capacidad de encriptar el tráfico cuando se esté optimizando.		
	Deberán soportarse optimización adicional de protocolos al menos para HTTP, CIFS, MAPI y FTP		
Control de Endpoint:	La solución debe tener la capacidad de definir políticas que permitan analizar el estado de las estaciones de trabajo antes de permitir el acceso.		
	Debe poder verificarse al menos los siguientes puntos:		
	Firewall personal instalado y activo		
	Antivirus instalado y con versión de firmas actualizadas		
	La solución debe poder controlar las aplicaciones en la estación de trabajo. Como evaluación de la política deberá ser capaz de determinar si una aplicación debe estar instalada, no instalada, ejecutándose o no ejecutándose.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Ante el incumplimiento de políticas la solución debe ofrecer la capacidad de bloquear el tráfico de dicho usuario o sólo alertarlo sobre el mismo.		
	La solución debe brindar la posibilidad de redireccionar el tráfico a un portal de remediación, cuando no se cumpla con alguna política de control de endpoint.		
	La evaluación de políticas podrá aplicarse mediante la instalación de un agente en la estación de trabajo.		
	En caso de requerir un agente en la estación de trabajo, debe poder determinarse la mínima versión aceptada de dicho agente como parte de las políticas de endpoint.		
	Debe permitir la posibilidad de validar el estado de cumplimiento de políticas en el momento de establecer la sesión y periódicamente		
Filtraje de tráfico VoIP, Peer-to-Peer y Mensajería instantánea	Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).		
	El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella,		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	KaZaa, Skype y WinNY para Peer-to-peer.		
	En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.		
	La solución debe contar con un ALG (Application Layer Gateway) de SIP		
	Debe poder hacerse inspección de encabezados de SIP		
	Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP.		
	La solución debe soportar SIP HNT (Hosted NAT Transversal).		
Alta disponibilidad:	Posibilidad en FirewallSoporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.		
	Alta Disponibilidad en modo Activo-Pasivo		
	Alta Disponibilidad en modo Activo-Activo		
	Posibilidad de definir al menos dos interfaces para sincronía		
	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Será posible definir interfaces de gestión independientes para cada miembro en un cluster.		
Características de Administración:	Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS)		
	La interfaz gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.		
	Interfaz basada en línea de comando (CLI) para administración de la solución.		
	Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.		
	Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)		
	El administrador del sistema podrá tener las opciones incluídas de autenticarse vía password y vía certificados digitales.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.		
	El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS		
	El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningun software adicional		
	Soporte de SNMP versión 2		
	Soporte de SNMP versión 3		
	Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos		
	Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.		
	Soporte de Control de Acceso basado en roles, con capacidad de crear al		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	menos 6 perfiles para administración y monitoreo del Firewall.		
	Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.		
	Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.		
Virtualización:	El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains"		
	La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus		
	Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.		
	Cada instancia virtual debe poder tener un administrador independiente		
	La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red		
	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual		
	Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.		
	Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.		

2.12.3. Distribución

Planilla N° 17 - Especificaciones técnicas			
Equipo Switch de distribución			
Equipo Switch de distribución	**Características**	**El bien ofertado cumple con las especificaciones requeridas (si/no)**	**Especificaciones técnicas ofertadas**
Cantidad	(05) cinco		
Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Descripción	Switch LAN apilable de capa 2 y 3		
Características Principales			
Interfaces:	Puertos 10/100/1000 RJ-45: ≥24		
	Puertos SFP : ≥4		
	Puertos de apilamiento 10G: ≥2		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Rendimiento:	Capacidad de switching: ≥128 Gbps		
	Capacidad de forwarding: ≥65,5 Mpps		
	Tamaño maximo de trama: 9216 bytes		
	Memoria Flash: ≥ 128 MB		
	Memoria RAM: ≥ 512 MB SDRAM		
Confiabilidad:	Tiempo medio entre fallos (MTBF): > 272.000 horas		
Configuración de red:	Soporta Auto negociación 10/100/1000 Mbps		
	Soporta Auto MDI/MDIX		
	Soporta BOOTP/DHCP		
	Soporta DHCP relay		
	Cumple con IEEE 802.1AB LLDP con extensiones MED		
	Soporta Multiple VLAN Registration Protocol (MVRP)		
	Soporta GARP VLAN Registration Protocol (GVRP)		
	Soporta Auto QoS		
	Soporta Network Time Protocol (NTP)		
Alta disponibilidad:	ITU-T G.8032 Ethernet Ring Protection		
	Ring Rapid Spanning Tree Protocol (RRSTP)		
	IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
	IEEE 802.1D Spanning Tree Protocol (STP)		
	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)		
	IEEE 802.3ad Link Aggregation Control Protocol (LACP)		
	Dual-home link		
	Evita tormentas de broadcast, unicast desconocido y multicast		
	Transceivers intercambiables en caliente		
	Configuracion e imagen dual para proveer backup		
Control de acceso:	Autosensing 802.1X con soporte multi-client, multi-VLAN		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Autenticacion basada en MAC para hosts no 802.1x		
	Autenticacion IEEE 802.1X y basada en MAC		
	Secure Shell (SSH)		
	Cliente TACACS+		
	RADIUS centralizado		
	Lightweight Directory Access Protocol (LDAP)		
Seguridad avanzada:	Learned Port Security (LPS) o MAC address lockdown		
	DHCP Snooping, DHCP IP y Address Resolution Protocol (ARP)		
	Traffic Anomaly Detection (TAD)		
	ARP poisoning detection		
	IP Source Filtering		
	ACLs para eliminar trafico no deseado, filtrado en hardware basado en flujo		
	Soporte para Microsoft Network Access Protection (NAP)		
	Soporta Bridge Protocol Data Unit (BPDU)		
	Soporta STP Root Guard		
Calidad de servicio (QoS):	Colas de prioridad: Hasta 8 colas por puerto basadas en hardware		
	Priorización de tráfico: QoS basado en flujo con priorización interna y externa (re-marking)		
	Gestión de ancho de banda basado en flujo		
	Gestión de colas: Algoritmos de programación configurables, (SPQ), (WRR), (DRR)		
	Políticas de red LLDP para designación dinamica de VLAN-ID		
Ruteo L3:	Soporta ruteo estatico		
	Soporta Routing Information Protocol Next Generation (RIPng)		
	Soporta OSPF v3		
	BGP v4		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	VRRP v3		
	Soporta Neighbor Discovery Protocol (NDP)		
Multicast:	Soporta Internet Group Management Protocol (IGMP) v1/v2/v3 snooping		
	Soporta Protocol Independent Multicast-Sparse Mode (PIM-SM)/Protocol Independent Multicast-Dense Mode (PIM-DM)		
	Soporta Distance Vector Multicast Routing Protocol (DVMRP)		
	Soporta Multicast Listener Discovery (MLD) v1/v2 snooping		
Estandares IEEE:	IEEE 802.1D (STP)		
	IEEE 802.1p (CoS)		
	IEEE 802.1Q VLANs		
	IEEE 802.1ad Provider Bridges (Q-in-Q/VLAN stacking)		
	IEEE 802.1ag (Connectivity Fault Management)		
	IEEE 802.1ak (Multiple VLAN Registration Protocol)		
	IEEE 802.1s MSTP		
	IEEE 802.1w RSTP		
	IEEE 802.1X Port Based NAC		
	IEEE 802.3i 10Base-T		
	IEEE 802.3u Fast Ethernet		
	IEEE 802.3x (Flow Control)		
	IEEE 802.3z Gigabit Ethernet		
	IEEE 802.3ab 1000Base-T		
	IEEE 802.3ac VLAN Tagging		
	IEEE 802.3ad (Link Aggregation)		
	IEEE 802.3ae 10G Ethernet		
Instalación	Todos los trabajos serán ejecutados de acuerdo a las reglas del arte y presentarán, una vez terminados, un aspecto prolijo y mecánicamente resistente.		
	Proveer los accesorios necesarios para la realización de las tareas: cintas, tornillos, arandelas, etc.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Además de cumplir con lo establecido en la presente documentación, las instalaciones deberán ser ejecutadas en un todo de acuerdo con los reglamentos para instalaciones de los estándares internacionales.		
	Se deberá prever las perforaciones y el anclaje necesario del rack dentro de la estructura de piso técnico del DataCenter actual.		
Fabricación	Todos los equipos deben ser nuevos, de fabricación reciente, encontrarse en comercialización.		
Certificación de calidad	Certificación ISO 9000 para todos los materiales utilizados.		
Garantía	Soporte de atención, repuestos, Mano de Obra y mantenimiento correctivo a cargo del Oferente		
Autorización del Fabricante para presentar oferta y certificación técnica.	Autorización escrita para presentar oferta. Técnicos certificados por fabrica (presentar documentación)		

4. ESPECIFICACIONES TÉCNICAS PARA LA PLANILLA DEL MINISTERIO DE JUSTICIA Y TRABAJO

4.10. Equipos Activos

Se solicitan en este proyecto un Switch de Core, un Router/Firewall de Core y equipos de de Distribución LAN.

4.10.1. Núcleo

Planilla N° 29 - Especificaciones técnicas

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Equipo Switch de core			
Equipo Switch de core	**Características**	**El bien ofertado cumple con las especificaciones requeridas (si/no)**	**Especificaciones técnicas ofertadas**
Cantidad	(01) uno		
Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Descripción	Switch de core		
Características Principales			
Fuente de Poder y redundancia	Dos, en modalidad redundante VAC 220 VAC @ 50 Hz.		
	Deberá soportar el intercambio de estas fuentes redundantes de poder en caliente, sin necesidad de bajar el equipo.		
	Deberá contar con 2 fuentes de poder trabajando en redundancia 1+1		
	Deberá contar con redundancia de cooling en la modalidad 3+1		
Interfaces	El equipo deberá poseer al menos 40 interfaces fijas SFP/SFP+ que soporten 1GbE/10GbE respectivamente con soporte de módulos ópticos y/o eléctricos intercambiables entre cualquiera de ellos.		
	El equipo deberá tener la capacidad de soportar hasta 64 interfaces de 10GbE SFP+ a través de módulos de expansión		
	El equipo deberá tener la capacidad de soportar al menos 6 interfaces de 40GbE a través de módulos QSFP+		
Soporte de protocolos de	1000Base-T		
	1000Base-SX		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

enlaces de Fibra Óptica y Cobre	1000Base-LX		
	1000Base-LH40		
	1000Base-LH70		
	10GbE-SR		
	10GbE-LR		
	10GbE-ER		
	10GbE-LRM		
	Todos los tipos de interfaces deben poder operar en modalidad Full Duplex.		
Transceivers solicitados	2 (uno) SFP+ 10 Gb Multimodo		
	2 (uno) SFP+ 10 Gb Monomodo		
	14 (Catorce) SFP Óptico Multimodo de 1 Gb		
	16 (Diez y Seis) SFP 1000BT (elecetrico)		
Del Sistema	Para la solución propuesta debe incluirse todo lo necesario para el correcto funcionamiento de todo el conjunto, es decir, accesorios y conexiones incluyendo a los equipos e instalaciones actuales.		
Switch Multilayer			
Alta Disponibilidad	El equipo básico debe disponer de un ancho de banda efectivo no menor a 1.2 Tbps provisto por un switching fabric no bloqueante.		
	Deberá tener capacidad de Alta disponibilidad en enlaces para los equipos conectados a estos switches a nivel de capa 2 a través de conexión de al menos 2 de estos switches de core brindando redundancia de enlaces del tipo Activo/Activo. No se aceptarán aplicaciones de Spanning Tree para este requerimiento. Ninguna		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	performance se deberá ver afectada con la caída de uno de los dos equipos trabajando en una de estas tecnologías citadas		
	El oferente deberá detallar y documentar mediante especificaciones técnicas originales del fabricante el funcionamiento de la Alta Disponibilidad ó High Availability del equipo.		
Performance	900 Mpps de 64 bytes (700 Millones de paquetes por segundo de 64 bytes cada uno).		
	La latencia máxima de los paquetes de 64 bytes deberá ser de: 7 µs en Capas 2 y 3 sobre interfaces 10 Gbe.		
	Capacidad de memoria SDRAM		
	Capacidad de memoria FLASH		
	Tamaño de tabla de Mac Address en L2		
	Tamaño de tabla de IPv4 en L3		
	Tamaño de tabla de IPv6 en L3		
	Tamaño de tabla para grupos MCAST		
	Tamaño de tablas para ACL		
	Tamaño de tablas para Link Aggregation: 32 grupos trunks, 2 a 8 puertos por grupos de trunk		
Características Adicionales del Equipo			
Normas ó recomendaciones	IEEE 802.1d		
	IEEE 802.1p		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

internacionales	IEEE 802.1q VLAN tagging (La cantidad de VLANs IDs no podrá ser inferior a 4.000).		
	IEEE 802.1s Per-VLAN Group Spanning Tree Protocol.		
	IEEE 802.1w RSTP.		
	IEEE 802.1x IBNS-Identity Based Networking Services.		
	IEEE 802.3ad Link aggregation control protocol.		
	IEEE 802.3ab 1000BASE-T.		
	IEEE 802.3ae 10 Gigabit Ethernet.		
	IEEE 802.3z 1000BaseSX/ 1000BaseLX/100BaseLH.		
	RFC 768 User Datagram Protocol (UDP).		
	RFC 783 Trivial File Transfer Protocol (TFTP).		
	RFC 791 IP.		
	RFC 792 Internet Control Message Protocol (ICMP).		
	RFC 793 TCP.		
	RFC 826 Address Resolution Protocol (ARP).		
	RFC 854 Telnet.		
	RFC 894 IP over Ethernet.		
	RFC 903 Reverse Address Resolution Protocol (RARP).		
	RFC 906 TFTP Bootstrap.		
	RFC 951, 1542 BOOTP, BOOTP extensions.		
	RFC 1027 Proxy ARP.		
	RFC 1122 Host requirements.		
	RFC 1519 Classless interdomain routing (CIDR).		
	RFC 1886 Domain Name System (DNS)		
	RFC 1812 IPv4.		
	RFC 2131 BOOTP/DHCP.		
	RFC 2338 VRRP.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	RFC 1112 Internet Group Management Protocol (IGMP).		
	RFC 2236 IGMP v1, v2, v3 snooping.		
	RFC 1583 OSPFv2.		
	RFC 1587 OSPF NSSA.		
	RFC 1745		
	RFC 1765 OSPF database overflow.		
	RFC 1850 OSPFv2 Management Information Base (MIB), traps.		
	RFC 1997 BGP Communities and attributes.		
	RFC 2154 OSPF digital signatures, MD5.		
	RFC 2370 OSPF opaque link-state advertisement (LSA) option.		
	RFC 1058 RIPv1.		
	RFC 2453 RIPv2.		
	RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6, and Open Systems Interconnection (OSI)		
	RFC 854 Telnet.		
	RFC 951 BOOTP.		
	RFC 1213 SNMP MIB II.		
	RFC 1724 RIPv2 MIB.		
	RFC 3418 SNMPv2c.		
	RFC 1492 TACACS+.		
	RFC 2865 RADIUS authentication.		
	SPAN.		
	Control y bloqueo de Media Access Control (MAC) address para seguridad.		
	RADIUS accounting		
	Autenticación vía RADIUS por cada comando.		
	Limite de ancho de banda real por cualquier criterio de Capas 2.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Se hace especial hincapié en el soporte de QoS, el equipo debe soportar el marcado, re-marcado, priorización y tratamiento de paquetes en distintas calidades de servicio por cualquier criterio de Capas 1, 2, 3 y 4 sin que ello afecte la performance del equipo (Ver especificaciones de performance y su impacto ante la aplicación de las distintas políticas de QoS).		
	El equipo debe soportar el manejo de frames ó tramas Ethernet de tamaño mayor al Standard específicamente debe soportar Jumbo Frames de 9.216 bytes y Giant babies de 1600 bytes.		
	RFC 3768 Virtual Router Redundancy Protocol		
Normas o reglamentaciones internacionales Adicionales	RFC 1771 BGP4.		
	RFC 1965 BGP4 autonomous system confederations.		
	RFC 2796 BGP4 route reflection.		
	RFC 1997 Communities attribute.		
	RFC 2385 Transmission Control Protocol (TCP) Message Digest Algorithm 5 (MD5) authentication for BGP.		
	RFC 2439 Route flap dampening.		
	RFC 2796 Route reflection.		
	RFC 2842 Capabilities advertisement.		
	RFC 2068 HTTP.		
	DHCP Server.		
	DHCP Server por VLAN		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Los equipos deben disponer de interfaces de salida que operen en 2da. Ventana (~1310nm) y 3ra. Ventana (~1550nm) compatible con la norma G.652.		
	El equipo soportará la facilidad de IGMP "snooping".		
	El equipo debe soportar la posibilidad de la sincronización horaria de los diferentes nodos de red.		
	El equipo debe disponer de interfaces virtuales con las mismas funcionalidades de las interfaces físicas.		
	El equipo debe permitir establecer direcciones IP secundarias (adicionales) en sus interfaces.		
Tráfico y Calidad de Servicio	Soporte de sumarización de rutas y redes (CIDR).		
	Prioridad de colas: 8 colas por puerto basado en hardware		
	Priorización de tráfico: QoS basado en tráfico		
	Gestión de control de ancho de banda basado en flujo		
	gestión de colas con configuración de agendamiento de algoritmos		
	RED, WRED		
	Arquitectura DiffServ		
Administración	El equipo debe disponer de un puerto serial RS-232 para conectar la gestión local, en caso de ser propietario, deben contar con su correspondiente adaptador.		
	El equipo en su gestión local debe disponer un mínimo de 3 niveles de acceso de usuario con diferentes atributos de modificación.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El nivel más alto de gestión local debe poder definir la lista de usuarios con su clave de acceso (password de al menos 8 caracteres) y sus atributos asociados.		
	Las claves de acceso (password) que contenga el equipo deben estar encriptados y no serán visibles por ningún comando de visualización.		
	Dentro de las prestaciones de la gestión local se debe disponer de un comando de visualización de eventos (log) encolados por aparición (tipo FIFO).		
	El equipamiento debe poder ser administrado/gestionado por los protocolos SNMPv1, SNMPv2, SNMPv3, RMON.		
	Deberá ser accesible local y remotamente con las mismas facilidades en ambas modalidades mediante protocolos seguros de comunicación, como mínimo SSH.		
	Deberá poder ser 100% administrable remotamente, pudiendo efectuar actualizaciones remotas de su sistema operativo sin que se interrumpa la comunicación con la estación de gerenciamiento y management.		
Instalación	Todos los trabajos serán ejecutados de acuerdo a las reglas del arte y presentarán, una vez terminados, un aspecto prolijo y mecánicamente resistente.		
	Proveer los accesorios necesarios para la realización de las tareas: cintas,		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	tornillos, arandelas, etc.		
	Además de cumplir con lo establecido en la presente documentación, las instalaciones deberán ser ejecutadas en un todo de acuerdo con los reglamentos para instalaciones de los estándares internacionales.		
	Se deberá prever las perforaciones y el anclaje necesario del rack dentro de la estructura de piso técnico del Data Center actual.		
Demostración	Se reserva el derecho de solicitar una demostración del equipo ofertado si fuese necesario.		
MTBF	140.000 horas		
Fabricación	Todos los equipos deben ser nuevos, de fabricación reciente, encontrarse en comercialización.		
Certificación de calidad	Certificación ISO 9000 para todos los materiales utilizados.		
Garantía	Soporte de atención, repuestos, Mano de Obra y mantenimiento correctivo a cargo del Oferente		
Autorización del Fabricante para presentar oferta y certificación técnica.	Autorización escrita para presentar oferta. Técnicos certificados por fabrica (presentar documentación)		

4.10.2. Firewall de Core

Planilla N° 30 - Especificaciones técnicas
Equipo Router/Firewall de core

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Equipo Router/Firewall de core	**Características**	**El bien ofertado cumple con las especificaciones requeridas (si/no)**	**Especificaciones técnicas ofertadas**
Cantidad	(01) uno		
Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Descripción	Router/Firewall de core		
Características Principales			
Definición:	Sistema de Seguridad informática que sea del tipo Administración Unificada de Amenazas, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que abajo se detallan, pudiendo ser todas ellas en una sola caja o en cajas diferentes.		
Funcionalidades y características del sistema			
Características de Desempeño:	Throughput Firewall @64/512/1500 Bytes: 20 Gbps		
	Throughput IPsec VPN: 8 Gbps		
	Throughput IPS: 6 Gbps		
	Throughput AV: 2.1 Gbps		
	Sesiones concurrentes: 7 Mil		
	Nuevas sesiones por segundo: 190.000		
Características de Hardware:	Interfaces GigaEthernet 10/100/1000: 12		
	Interfaces 10GigE: 2 SFP+		
	Almacenamiento Tamaño (GB): 128 GB		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Características del dispositivo:	El dispositivo debe ser una appliance de propósito específico		
	Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.		
	Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).		
	Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).		
	El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red.		
	En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Características del Sistema operativo incluido:	Sistema operativo pre-endurecido específico para seguridad que sea compatible con el appliance. Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows		
	El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.		
Firewall:	Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs		
	Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.		
	Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando		
	Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.		
	Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación		
	Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.		
	Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo		
	Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)		
	Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.		
	Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.		
	Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.		
	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)		
	La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas		
	En la solución de balanceo de carga entre servidores, debe soportarse persitencia de sesión al menos mediante HTTP Cookie o SSL Session ID		
	En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.		
Conectividad y sistema de ruteo:	Se debe considerar al menos el tener una interface/puerto DMZ y 2 puertos para enlaces WAN.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP		
	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs		
	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas		
	Soporte a políticas de ruteo (policy routing)		
	El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace		
	Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS		
	Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+		
	La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.		
	Soporte de ECMP (Equal Cost Multi-Path)		
	Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.		
	Soporte a ruteo de multicast		
	La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.		
VPN Ipsec/L2TP/PPTP:	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)		
	Soporte para IKEv2 y IKE Configuration Method		
	Debe soportar la configuración de túneles L2TP		
	Debe soportar la configuración de túneles PPTP		
	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.		
	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits		
	Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.		
	Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.		
	Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.		
	La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)		
	En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.		
	Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.		
	Capacidad minima de tuneles - GW to GW (10.000 tunel IPsec) - GW to client (50.000 tunel IPsec)		
VPN SSL:	Capacidad de realizar SSL VPNs.		
	Soporte a certificados PKI X.509 para construcción de VPNs SSL.		
	Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.		
	Soporte de renovación de contraseñas para LDAP y		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	RADIUS.		
	Soporte a asignación de aplicaciones permitidas por grupo de usuarios		
	Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.		
	Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.		
	Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)		
	La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS		
	Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL		
	Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.		
	Los portales personalizados deberán soportar al menos la definición de:		
	Widgets a mostrar		
	Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC		
	Esquema de colores		
	Soporte para Escritorio Virtual		
	Política de verificación de la estación de trabajo.		
	La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.		
	En la configuración del Escritorio Virtual podrá definirse como mínimo:		
	La posibilidad de que el usuario cambie entre escritorio virtual y real.		
	La posibilidad de restringir el acceso a la memoria (clipboard) del escritorio virtual desde el escritorio real.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	La posibilidad de utilizar medios removibles desde el escritorio virtual		
	La posibilidad de acceder a recursos compartidos desde el escritorio virtual		
	La posibilidad de imprimir desde el escritorio virtual.		
	La posibilidad de definir y restringir las aplicaciones que podrán ser ejecutadas en el escritorio virtual.		
Traffic Shapping / QoS:	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall		
	Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión		
	Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.		
	Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo		
	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo		
	Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Capacidad de integrarse con Servidores de Autenticación RADIUS.		
	Capacidad nativa de integrarse con directorios LDAP		
	Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"		
Autenticación y Certificación Digital:	Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.		
	Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.		
	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)		
	Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.		
	Soporte de verificación de validación de certificados digitales mediante el		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	protocolo OSCP (Online Simple Enrrollment Protocol)		
	La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.		
	Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.		
	Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:		
	Longitud mínima permitida		
	Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.		
	Expiración de contraseña.		
	Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP		
Antivirus:	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.		
	Antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.		
	El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.		
	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.		
	El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List)		
	El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP		
	El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.		
	El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.		
	El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.		
	El antivirus deberá ser capaz de filtrar archivos por extensión		
	El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)		
Antispam:	La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.		
	La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)		
	La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	mecanismos para detección de SPAM		
	En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.		
Filtraje de URLs (URL Filtering):	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.		
	Debe poder categorizar contenido Web requerido mediante IPv6.		
	Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.		
	Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida		
	Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.		
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).		
	La solución de Filtraje de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.		
	Será posible exceptuar la inspección de HTTPS por categoría.		
IPS:	El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de linea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror		
	El detector y preventor de intrusos podrá implementarse en linea y fuera de linea en forma simultánea para distintos segmentos.		
	Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6		
	Capacidad de detección de más de 4000 ataques.		
	Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	El Detector y preventor de intrusos deberá de estar orientado para la protección de redes.		
	El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.		
	El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).		
	Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.		
	Tecnología de detección tipo Stateful basada en Firmas (signatures).		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Actualización automática de firmas para el detector de intrusos		
	El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.		
	Mecanismos de detección de ataques: § Reconocimiento de patrones, Análisis de protocolos, § Detección de anomalías § Detección de ataques de RPC (Remote procedure call) § Protección contra ataques de Windows o NetBios § Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol) § Protección contra ataques DNS (Domain Name System) § Protección contra ataques a FTP, SSH , Telnet y rlogin § Protección contra ataques de ICMP (Internet Control Message Protocol).		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Métodos de notificación: § Alarmas mostradas en la consola de administración del appliance. § Alertas vía correo electrónico. § Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque.Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. § La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto.		
	Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP		
Prevención de Fuga de Información (DLP):	La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.		
	Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.		
	Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento,		
	En caso del bloqueo de usuarios, la solución debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.		
	La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.		
	La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.		
Control de Aplicaciones:	Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.		
	Las solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.		
	El listado de aplicaciones debe actualizarse periódicamente.		
	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.		
	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.		
	Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.		
	Preferentemente deben soportar mayor granularidad en las acciones.		
Inspección de Contenido SSL:	La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.		
	La inspección deberá realizarse mediante la técnica conocida como		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Hombre en el Medio (MITM – Man In The Middle).		
	La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.		
	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.		
Cache Web:	La solución debe soportar actuar como un cache web, entendiéndose como la capacidad de almacenar contenido estátic que será servido localmente en posteriores requerimientos.		
	Debe poder definirse el tamaño del almacenamiento dedicado para la función de web cache.		
	Debe poder definirse el máximo tiempo en el que un objeto permanecerá en el caché (TTL).		
	El web cache debe configurarse mediante reglas que definirán el contenido que debe ser almacenado al menos con los siguientes parámetros: Dirección IP o grupo de direcciones IP de origen,		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	dirección IP o grupo de direcciones IP de destino, rango de puertos de destino.		
	El Cache Web podrá configurarse en forma transparente. En este modo, no es necesario que el navegador del usuario tenga configurado un Proxy.		
	El Caché Web podrá configurarse como un Proxy HTTP explícito en la red. Esto significa que los navegadores podrán configurar el dispositivo FortiGate como Proxy para la navegación.		
	Soporte del protocolo WCCPv2. Este protocolo debe soportarse en modo cliente como en modo servidor. En modo servidor, el dispositivo será capaz de redireccionar el tráfico Web hacia uno o más servidores de Caché Web en modo transparente para el usuario final. En modo cliente, el dispositivo podrá comportase como un Web Caché al cual se le redireccionará tráfico por un servidor de WCCPv2		
	WCCPv2 deberá soportarse tanto con GRE como Layer 2 forwarding.		
	La solución debe soportar la capacidad de aplicar el Caché Web a tráfico		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	encriptado con SSL (HTTPS).		
	Cuando la solución se encuentre configurada como un Proxy explícito, éste debe poder habilitarse de forma diferenciada por interfaz de red.		
	En Proxy explícito la solución debe soportar los siguientes protocolos: HTTP, HTTPS, FTP y SOCKS		
	En Proxy explícito debe poder configurarse de forma independiente los puertos en los que estarán activos los siguientes protocolos: HTTP, HTTPS, FTP y SOCKS.		
	En Proxy explícito la solución debe soportar la configuración automática de los navegadores mediante PAC File (Proxy Auto-Configuration File)		
Optimización de WAN	La solución deberá soportar la capacidad de disminuir el tráfico transmitido por un determinado enlace mediante diferentes técnicas.		
	El Optimización de WAN debe configurarse mediante reglas que definirán el tráfico a optimizar al menos con los siguientes parámetros: Dirección IP o grupo de direcciones IP de origen, dirección IP o grupo de direcciones IP de destino, rango de puertos de destino.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Deberán utilizarse al menos las siguientes técnicas para Optimización WAN: Compresión, Byte Caching, Object Caching		
	En caso de requerirse un dispositivo en ambos extremos del enlace de comunicaciones, debe ser posible autenticar las partes antes de establecer la optimización		
	La solución debe tener la capacidad de encriptar el tráfico cuando se esté optimizando.		
	Deberán soportarse optimización adicional de protocolos al menos para HTTP, CIFS, MAPI y FTP		
Control de Endpoint:	La solución debe tener la capacidad de definir políticas que permitan analizar el estado de las estaciones de trabajo antes de permitir el acceso.		
	Debe poder verificarse al menos los siguientes puntos:		
	Firewall personal instalado y activo		
	Antivirus instalado y con versión de firmas actualizadas		
	La solución debe poder controlar las aplicaciones en la estación de trabajo. Como evaluación de la política deberá ser capaz de determinar si una aplicación debe estar instalada, no instalada, ejecutándose o no ejecutándose.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Ante el incumplimiento de políticas la solución debe ofrecer la capacidad de bloquear el tráfico de dicho usuario o sólo alertarlo sobre el mismo.		
	La solución debe brindar la posibilidad de redireccionar el tráfico a un portal de remediación, cuando no se cumpla con alguna política de control de endpoint.		
	La evaluación de políticas podrá aplicarse mediante la instalación de un agente en la estación de trabajo.		
	En caso de requerir un agente en la estación de trabajo, debe poder determinarse la mínima versión aceptada de dicho agente como parte de las políticas de endpoint.		
	Debe permitir la posibilidad de validar el estado de cumplimiento de políticas en el momento de establecer la sesión y periódicamente		
Filtraje de tráfico VoIP, Peer-to-Peer y Mensajería instantánea	Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).		
	El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella,		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	KaZaa, Skype y WinNY para Peer-to-peer.		
	En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.		
	La solución debe contar con un ALG (Application Layer Gateway) de SIP		
	Debe poder hacerse inspección de encabezados de SIP		
	Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP.		
	La solución debe soportar SIP HNT (Hosted NAT Transversal).		
Alta disponibilidad:	Posibilidad en FirewallSoporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.		
	Alta Disponibilidad en modo Activo-Pasivo		
	Alta Disponibilidad en modo Activo-Activo		
	Posibilidad de definir al menos dos interfaces para sincronía		
	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Será posible definir interfaces de gestión independientes para cada miembro en un cluster.		
Características de Administración:	Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS)		
	La interfaz gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.		
	Interfaz basada en línea de comando (CLI) para administración de la solución.		
	Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.		
	Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)		
	El administrador del sistema podrá tener las opciones incluídas de autenticarse vía password y vía certificados digitales.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.		
	El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS		
	El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningun software adicional		
	Soporte de SNMP versión 2		
	Soporte de SNMP versión 3		
	Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos		
	Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.		
	Soporte de Control de Acceso basado en roles, con capacidad de crear al		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	menos 6 perfiles para administración y monitoreo del Firewall.		
	Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.		
	Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.		
Virtualización:	El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains"		
	La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus		
	Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.		
	Cada instancia virtual debe poder tener un administrador independiente		
	La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red		
	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual		
	Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.		
	Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.		

4.10.3. Distribución

Planilla N° 31 - Especificaciones técnicas			
Equipo Switch de distribución			
Equipo Switch de distribución	**Características**	**El bien ofertado cumple con las especificaciones requeridas (si/no)**	**Especificaciones técnicas ofertadas**
Cantidad	(05) cinco		
Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Descripció	Switch LAN apilable de capa 2 y 3		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

n			
Caracteristicas Principales			
Interfaces:	Puertos 10/100/1000 RJ-45: ≥24		
	Puertos SFP: ≥4		
	Puertos de apilamiento 10G: ≥2		
Rendimiento:	Capacidad de switching: ≥128 Gbps		
	Capacidad de forwarding: ≥65,5 Mpps		
	Tamaño maximo de trama: 9216 bytes		
	Memoria Flash: ≥ 128 MB		
	Memoria RAM: ≥ 512 MB SDRAM		
Confiabilidad:	Tiempo medio entre fallos (MTBF): > 272.000 horas		
Configuración de red:	Soporta Auto negociación 10/100/1000 Mbps		
	Soporta Auto MDI/MDIX		
	Soporta BOOTP/DHCP		
	Soporta DHCP relay		
	Cumple con IEEE 802.1AB LLDP con extensiones MED		
	Soporta Multiple VLAN Registration Protocol (MVRP)		
	Soporta GARP VLAN Registration Protocol (GVRP)		
	Soporta Auto QoS		
	Soporta Network Time Protocol (NTP)		
Alta disponibilidad:	ITU-T G.8032 Ethernet Ring Protection		
	Ring Rapid Spanning Tree Protocol (RRSTP)		
	IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
	IEEE 802.1D Spanning Tree Protocol (STP)		
	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)		
	IEEE 802.3ad Link Aggregation Control Protocol (LACP)		
	Dual-home link		
	Evita tormentas de broadcast, unicast desconocido y multicast		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

	Transceivers intercambiables en caliente		
	Configuracion e imagen dual para proveer backup		
Control de acceso:	Autosensing 802.1X con soporte multi-client, multi-VLAN		
	Autenticacion basada en MAC para hosts no 802.1x		
	Autenticacion IEEE 802.1X y basada en MAC		
	Secure Shell (SSH)		
	Cliente TACACS+		
	RADIUS centralizado		
	Lightweight Directory Access Protocol (LDAP)		
Seguridad avanzada:	Learned Port Security (LPS) o MAC address lockdown		
	DHCP Snooping, DHCP IP y Address Resolution Protocol (ARP)		
	Traffic Anomaly Detection (TAD)		
	ARP poisoning detection		
	IP Source Filtering		
	ACLs para eliminar trafico no deseado, filtrado en hardware basado en flujo		
	Soporte para Microsoft Network Access Protection (NAP)		
	Soporta Bridge Protocol Data Unit (BPDU)		
	Soporta STP Root Guard		
Calidad de servicio (QoS):	Colas de prioridad: Hasta 8 colas por puerto basadas en hardware		
	Priorización de tráfico: QoS basado en flujo con priorización interna y externa (re-marking)		
	Gestión de ancho de banda basado en flujo		
	Gestión de colas: Algoritmos de programación configurables, (SPQ), (WRR), (DRR)		
	Políticas de red LLDP para designación dinamica de VLAN-ID		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Ruteo L3:	Soporta ruteo estatico		
	Soporta Routing Information Protocol Next Generation (RIPng)		
	Soporta OSPF v3		
	BGP v4		
	VRRP v3		
	Soporta Neighbor Discovery Protocol (NDP)		
Multicast:	Soporta Internet Group Management Protocol (IGMP) v1/v2/v3 snooping		
	Soporta Protocol Independent Multicast-Sparse Mode (PIM-SM)/Protocol Independent Multicast-Dense Mode (PIM-DM)		
	Soporta Distance Vector Multicast Routing Protocol (DVMRP)		
	Soporta Multicast Listener Discovery (MLD) v1/v2 snooping		
Estandares IEEE:	IEEE 802.1D (STP)		
	IEEE 802.1p (CoS)		
	IEEE 802.1Q VLANs		
	IEEE 802.1ad Provider Bridges (Q-in-Q/VLAN stacking)		
	IEEE 802.1ag (Connectivity Fault Management)		
	IEEE 802.1ak (Multiple VLAN Registration Protocol)		
	IEEE 802.1s MSTP		
	IEEE 802.1w RSTP		
	IEEE 802.1X Port Based NAC		
	IEEE 802.3i 10Base-T		
	IEEE 802.3u Fast Ethernet		
	IEEE 802.3x (Flow Control)		
	IEEE 802.3z Gigabit Ethernet		
	IEEE 802.3ab 1000Base-T		
	IEEE 802.3ac VLAN Tagging		
	IEEE 802.3ad (Link Aggregation)		
	IEEE 802.3ae 10G Ethernet		

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones

Instalación	Todos los trabajos serán ejecutados de acuerdo a las reglas del arte y presentarán, una vez terminados, un aspecto prolijo y mecánicamente resistente.		
	Proveer los accesorios necesarios para la realización de las tareas: cintas, tornillos, arandelas, etc.		
	Además de cumplir con lo establecido en la presente documentación, las instalaciones deberán ser ejecutadas en un todo de acuerdo con los reglamentos para instalaciones de los estándares internacionales.		
	Se deberá prever las perforaciones y el anclaje necesario del rack dentro de la estructura de piso técnico del DataCenter actual.		
Fabricación	Todos los equipos deben ser nuevos, de fabricación reciente, encontrarse en comercialización.		
Certificación de calidad	Certificación ISO 9000 para todos los materiales utilizados.		
Garantía	Soporte de atención, repuestos, Mano de Obra y mantenimiento correctivo a cargo del Oferente		
Autorización del Fabricante para presentar oferta y certificación técnica.	Autorización escrita para presentar oferta. Técnicos certificados por fabrica (presentar documentación)		

----------//----------

Fin de las modificaciones

Se remite la presente Addenda, como complemento del Pliego de Bases y Condiciones, la cual pasa a formar parte del mismo y deberá presentarse como contenido de la carpeta de oferta, debidamente numerado y rubricado por el Representante de la firma oferente.

Abg. Elizabeth Schecht Pfefferkorn
Directora de Contrataciones