Detalle de los productos con las respectivas especificaciones técnicas

LOTE N° 1 - ADQUISICIÓN DE SWITCHES				
ITEM	**DESCRIPCIÓN**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**PRESENTACIÓN**
1	SWITCHES DE CORE	2	UNIDAD	UNIDAD
2	SWITCHES DE DATA CENTER	3	UNIDAD	UNIDAD
3	SWITCHES DE ACCESO	20	UNIDAD	UNIDAD
LOTE N° 2 – ADQUISICIÓN DE EQUIPOS DE SEGURIDAD FORTINET				
1	SOLUCIÓN ANTISPAM Y SEGURIDAD PARA CORREO **FORTINET FORTIMAIL**	2	UNIDAD	UNIDAD
2	CORTAFUEGOS DE APLICACIONES WEB **FORTINET FORTIWEB**	2	UNIDAD	UNIDAD

Alcance de los trabajos y servicios

Los oferentes deberán entregar todos los bienes y servicios del presente llamado en la modalidad de llave en mano, por lo que deberán considerar todos los equipamientos, accesorios, materiales de instalación, horas de servicio técnico especializado, etc., para la correcta implementación de la solución ofertada, de acuerdo con los requerimientos técnicos indicados en el presente documento.

Entre los servicios que se identifican y se mencionan de manera enunciativa pero no taxativa se encuentran:

- Desinstalar y desmontar los equipos actualmente utilizados y ubicados en sus respectivos gabinetes.
- Instalar y conectorizar todos los nuevos equipos adquiridos.
- Actualizar el sistema operativo de los equipos proveídos a la última versión disponible.
- Arreglar, reemplazar, etiquetar y/o identificar los cables, para el correcto montaje de los nuevos equipos.
- Configurar los nuevos equipos montados y los ya existentes, a fin de lograr la interconexión necesaria para el uso y acceso a la red y servicios.
- Todos los dispositivos conectados deberán contar con enlaces redundantes para prevenir interrupciones en el servicio.
- Documentación técnica que contenga el diagrama físico, diagrama lógico, etiquetado y certificación del esquema del despliegue de la red de datos.
- Realizar la transferencia tecnológica por cada ítem solicitado.

- Además, los switches del LOTE 1 – ITEM 1,2 Y 3 deberán ser de la misma marca o fabricante de tal manera a garantizar interoperabilidad y gestión unificada centralizada.

Se debe considerar que los equipos montados, deberán contar con un servicio de mantenimiento preventivo y correctivo, de manera local, por el plazo del contrato (36 meses).

El proveedor deberá prever horas/técnico bajo demanda, de acuerdo con las necesidades de la entidad convocante, con el fin de atender reclamos, realizar configuraciones adicionales o abordar cualquier otra necesidad identificada y requerida.

Corresponde mencionar que los servicios de instalación, montaje, configuración y todo lo necesario para la puesta en funcionamiento de los equipos e infraestructura de red de datos deberán ser realizados por los técnicos propuestos, cuya documentación fuera proveída en el momento de la oferta, salvo casos excepcionales y debidamente justificados. Para estos casos, el técnico propuesto por la empresa deberá tener el mismo o mejor perfil que el reemplazado y estará sujeto a aprobación por parte de la Convocante.

Asimismo, el proveedor se compromete a reemplazar partes cambiables de los equipos que presenten fallas identificadas, como, por ejemplo, fuentes de poder, módulos de expansión, GBIC's, SFP, etc.

Por lo que se requiere lo detallado a continuación:

LOTE N° 1 - ADQUISICIÓN DE SWITCHES

ITEM N° 1: Switch de CORE

Se deberá contemplar la provisión de 2 (dos) switches de core administrables de 24 puertos a 10Gbase X con 2 puertos uplink a 100 GB cada uno, módulos o adaptadores para disponibilizar el stack o apilamiento (vss, virtual chassis o semejante) y módulos SFP+ 10 GB para los enlaces verticales de FO (switches de acceso, proveedores y data center) y dispositivos de seguridad (cortafuegos WAF y seguridad de correo) **(ÍTEM 4 y 5).**

Los equipos suministrados deberán configurarse en un esquema de alta disponibilidad (HA), garantizando la continuidad de la operatividad de la red en caso de que uno de los switches presente una falla.

ITEM N°2: Switch de DATA CENTER

Se deberá contemplar la provisión de 3 (tres) switches administrables de 48 puertos cada uno, cuatro interfaces de uplink, módulos o adaptadores para disponibilizar el stack o apilamiento (vss, virtual chassis o semejante) y módulos SFP+ 10GB para los enlaces de FO con los Switches de CORE **(ITEM 1)**.

ITEM N° 3: Switches de ACCESO

Se deberá contemplar la provisión de 20 (veinte) switches administrables de acceso de 48 puertos cada uno, cinco de ellos con soporte POE, cuatro interfaces de uplink a 10 GB, módulos o adaptadores para disponibilizar el stack o apilamiento (vss, virtual chassis o semejante) y módulos SFP+ 10 GB para los enlaces verticales a través de FO a los Switches CORE **(ITEM 1)**.

Ubicación	Cantidad		Subtotal
	Sin POE	Con POE	
PLANTA BAJA	4	1	5
ENTREPISO	3	1	4
PRIMER PISO	6	1	7
SEGUNDO PISO	1	1	2
TERCER PISO	0	1	1
CUARTO PISO	0	1	1
TOTAL	**14**	**6**	**20**

Observaciones:

Actualmente ya se encuentran desplegados los enlaces verticales a los distintos pisos a través de fibra óptica multimodo, todos conectorizados a sus respectivos DIO.

LOTE N° 2 – ADQUISICIÓN DE EQUIPOS DE SEGURIDAD FORTINET

ITEM N° 1 : Solución antispam y seguridad para correo electrónico

Se requieren 02 (dos) dispositivos capaces de ofrecer una robusta solución para garantizar la integridad y confidencialidad de las comunicaciones electrónicas en la Institución. A continuación, se presentan detalles, descripciones y características claves que deben cumplir los equipos.

Seguridad Integral: Defensa integral contra las amenazas de correo electrónico, incluyendo malware, phishing y ataques dirigidos.

Filtrado Avanzado: Técnicas de filtrado para detectar y bloquear correos no deseados y peligrosos.

Análisis Heurístico: Para identificar amenazas desconocidas basadas en comportamientos sospechosos.

Detección de Contenido: Escanea los mensajes en busca de contenido sensible o violaciones de políticas predefinidas.

Prevención de Fuga de Datos: Protege a la organización contra la fuga de información confidencial a través del correo electrónico.

Rendimiento Eficiente: Alto rendimiento para gestionar grandes volúmenes de correos electrónicos de manera eficiente.

Alta Disponibilidad: Garantizar la disponibilidad continua del servicio de correo electrónico para evitar interrupciones en la comunicación (HA).

Actualizaciones en Tiempo Real: Mantener una base de datos actualizada de amenazas para una protección en tiempo real.

Gestión Centralizada: Administración centralizada de políticas de seguridad de correo electrónico.

Informes Detallados: Informes detallados sobre el tráfico de correo y las amenazas bloqueadas.

Estas características son requeridas con el objeto de salvaguardar la integridad y seguridad de la comunicación por correo electrónico, brindando una protección confiable y actualizada contra las crecientes amenazas cibernéticas.

Ambos dispositivos se deben de configurar en un esquema de Alta Disponibilidad (HA) en caso de que uno de los mismos presente una falla.

Para garantizar la compatibilidad de las funciones requeridas, el equipo deberá ser del mismo fabricante del actual **FIREWALL/UTM** y **ANALIZADOR DE LOGS** con que cuenta la Institución, **FORTINET FORTIGATE 200F y FORTIANALYZER VM**, o en su defecto contar con un respaldo documental de interoperabilidad de las funciones de administración centralizada, de gestión de reportes, entre otros. Es decir, ambos fabricantes deberán garantizar mediante nota dirigida a la Convocante la interoperabilidad entre equipos.

ITEM N° 2: Cortafuegos de aplicaciones web

Se requieren 02 (dos) dispositivos capaces de brindar una solución de seguridad de red diseñada para proteger aplicaciones web críticas contra amenazas cibernéticas. Su enfoque está en garantizar la integridad, confidencialidad y disponibilidad de los datos que circulan a través de aplicaciones web. A continuación, se presentan detalles, descripciones y características claves que deben cumplir los equipos.

Protección en Tiempo Real: Defensa en tiempo real contra amenazas web, incluyendo ataques de inyección SQL, cross-site scripting (XSS), y otros ataques comunes.

Detección y Prevención de Ataques: Técnicas avanzadas de detección de intrusos para identificar y prevenir amenazas antes de que afecten las aplicaciones.

WAF (Web Application Firewall): Inspeccionar y filtrar tráfico HTTP/HTTPS para proteger aplicaciones contra ataques y vulnerabilidades conocidas.

Balanceo de Carga y Disponibilidad: Garantizar el acceso continuo a las aplicaciones, incluso en situaciones de alto tráfico.

Optimización de Rendimiento: Optimizar el rendimiento de aplicaciones web al reducir la latencia y acelerar la entrega de contenido.

Gestión Centralizada: Permitir una gestión centralizada y sencilla de las políticas de seguridad a través de una interfaz intuitiva.

Escalabilidad: Escalable para adaptarse a las necesidades de crecimiento de las aplicaciones y la red.

Integración de Informes y Análisis: Proporcionar informes detallados y herramientas de análisis para evaluar la eficacia de las políticas de seguridad.

Actualizaciones Continuas: Actualizaciones periódicas que mantienen la protección actualizada contra las amenazas emergentes.

Alta Disponibilidad: Ofrece opciones para configuraciones de alta disponibilidad, asegurando la continuidad de las operaciones.

Estas características son requeridas para contar con una solución sólida, garantizar la seguridad y el rendimiento de las aplicaciones web proveídas por la Institución.

Ambos dispositivos se deben de configurar en un esquema de Alta Disponibilidad (HA) en caso de que uno de los mismos presente una falla.

Para garantizar la compatibilidad de las funciones requeridas, el equipo deberá ser del mismo fabricante del actual **FIREWALL/UTM** y **ANALIZADOR DE LOGS** con que cuenta la Institución, **FORTINET FORTIGATE 200F y FORTIANALYZER VM**, o en su defecto contar con un respaldo documental de interoperabilidad de las funciones de administración centralizada, de gestión de reportes, entre otros. Es decir, ambos fabricantes deberán garantizar mediante nota dirigida a la Convocante la interoperabilidad entre equipos.

A continuación, se listan de manera enunciativa y no limitativa las Especificaciones Técnicas consideradas dentro del alcance del presente proyecto, donde todos los ítems y accesorios deberán ser compatibles entre sí, garantizando su correcta interoperabilidad:

LOTE N° 1 – ADQUISICIÓN DE SWITCHES

	ITEM 1 - SWITCHES DE CORE	
Nro.	**Descripción**	**Requerimiento mínimo exigido**
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	2 (dos)
5	Descripcion	Switch de Core
6	Stacking/Apilamiento: minima cantidad de equipos apilables	≥ 2
7	Tipo de uso	Core
	RENDIMIENTO Y CAPACIDAD	
8	Capacidad mínima de forwarding soportado por equipo	≥ 490Mpps
9	Capacidad mínima de conmutación soportada por equipo	≥ 1050 Gbps
10	Capacidad mínima de forwarding entre módulos o miembros del stacking (backplane) soportado por equipo	≥ 300 Gbps

11	El equipo deberá estar equipado con la cantidad de Memoria RAM y FLASH mínima necesaria para soportar todas las funcionalidades de la última versión del sistema operativo en el momento de la entrega del equipo y los requerimientos de prestaciones y performance solicitadas en estas especificaciones técnicas.	RAM/ DRAM ≥ 4GB
12	MTBF Mínimo Requerido	≥ 320.000 Hs.
	INTERFACES	
13	Cantidad mínima de interfaces 40/100GbE QSFP28 independientes instalados	≥ 2
14	Cantidad mínima de interfaces de 10 GbE ópticas instaladas (independientes de los items anteriores)	≥ 24
15	Capacidad de crecimiento mínima en interfaces de 10GbE y/o 25GbE	≥ 4 (opcional)
16	Cantidad mínima de puertos Serial independiente para administración fuera de banda del equipo.	≥ 1 (opcional)
17	Cantidad mínima de puertos RJ-45 para ser usado como consola de administración.	≥ 1
18	modulos SFP+ FO (a incluir) para velocidades 10Gbps	32 en total (16 por equipo)
19	patchcord FO (a incluir)	32 en total (16 por equipo)
	Stacking/Apilamiento	
20	Vinculación de equipos por puertos con interfaces que soporten mínimo 40GbE	EXIGIDO
21	Configuración desde una única dirección IP y para su administración actuarán como un único equipo.	EXIGIDO
22	El reemplazo de un miembro del stack deberá ser no disruptivo. En caso que la versión de Sistema Operativo del equipo a incorporar sea distinta de la vigente el stack/Virtual Chasis , la misma deberá poder actualizarse automáticamente desde el equipo controlador del stack/Master del Virtual Chasis	EXIGIDO
23	Capacidad de conformar un único equipo desde el punto de vista de la administración	EXIGIDO
24	Mínimo de equipos agrupados para administrar con un único acceso administrativo	≥ 4
25	Los puertos miembros de un grupo de Link Aggregation (802.3ad) LAG deben poder pertenecer a diferentes miembros del Stack	EXIGIDO
	FUNCIONES SWITCH DE RED	
26	Todas las interfaces se podrán utilizar independientemente en modo L3 o L2 , es decir se podrán agrupar para formar un dominio de Broadcast (L2) representadas por una interfase L3 virtual (Interfase VLAN) o cada interfase física o lógica podrá configurarse con una dirección IP independiente (L3)	EXIGIDO
27	Funcionalidad de Servidor DHCP	EXIGIDO
28	Funcionalidad de Cliente DHCP	EXIGIDO
29	Funcionalidad de DHCP Relay y Helper	EXIGIDO
30	Protocolo de enrutamiento RIPv1, RIPv2	EXIGIDO
31	Capacidad de soporte para Protocolo de enrutamiento OSPF v2, v3	EXIGIDO
32	Soporte de Bidirectional Forwarding Detection (BFD) con instalacion futura de licencia correspondiente	EXIGIDO
33	Soporte de protocolo de enrutamiento BGP	EXIGIDO
34	Soporte de protocolo de encapsulamiento VXLAN	EXIGIDO

35	Debe soportar la funcionalidad de ruteo por distintos campos del paquete IP como Origen/Destino o puertos (Policy Based Routing o Filter Based Routing) en forma independiente a la tabla de ruteo por defecto	EXIGIDO
36	Mínimo VLANS soportadas – 802.1q Vlan Tagging	≥ 4092
37	Mínimo de direcciones MAC	≥ 112000
38	Mínimo de rutas IPv4 unicast	≥ 130000
39	Mínimo de rutas multicast IPv4	40000
40	Multiple VLAN Registration Protocol (802.1ak)	EXIGIDO
	MULTICAST	
41	Los switches deberán tener la capacidad de interactuar con tráfico multicast para ello deberán soportar los siguientes protocolos :	EXIGIDO
42	IGMP Snooping	EXIGIDO
43	Capacidad de Soporte de IGMP v1 v2 y v3	EXIGIDO
44	Soporte PIM (Protocol Independant Multicast) en modo Sparse, SSM y DM	EXIGIDO
45	Capacidad de Soporte de protocolo MSDP (Multicast Source Discovery Protocol)	EXIGIDO
	ENRUTAMIENTO	
46	RIP v1 y v2	EXIGIDO
47	OSPF v2 y v3	EXIGIDO
48	BGP	EXIGIDO
49	VXLAN	EXIGIDO
	Management	
50	Syslog, Telnet, SSH	EXIGIDO
51	Neighbor DiscoveryProtocol	EXIGIDO
52	IPv6 ping	EXIGIDO
53	MLDv1 v2	EXIGIDO
	CALIDAD DE SERVICIO	
54	Mínimo de colas por hardware de calidad de servicio por interfase	12
55	Configuración por políticas de Calidad de Servicio asociando y marcando el tráfico a una determinada Clase de Servicio:	EXIGIDO
56	por Interfase	EXIGIDO
57	por dirección MAC	EXIGIDO
58	por campo 802.1p	EXIGIDO
59	por VLAN	EXIGIDO
60	por dirección IP origen y/o Destino	EXIGIDO
61	por campo DSCP/IP precedente	EXIGIDO
62	por puertos TCP/UDP	EXIGIDO
63	Configurar la Priorización del tráfico Saliente para cada clase de Servicio	EXIGIDO
	SEGURIDAD	
64	Limitar la cantidad de Direcciones MAC por puerto.	EXIGIDO
65	Deberá soportar MACSEC	EXIGIDO
66	Dynamic ARP inspection (DAI)	EXIGIDO
67	Deberá soportar Local Proxy ARP	EXIGIDO
68	Debera soportar Proxy ARP por VLAN	EXIGIDO
69	Deberá soportar DHCP Snooping	EXIGIDO

70	Deberá soportar Static ARP	EXIGIDO
	CONTROL DE ACCESO Y AUTENTICACION	
71	Cantidad mínima de ACL basadas en el puerto aplicadas al ingreso de los paquetes.	2048
72	Cantidad mínima de ACL basadas en el VLAN aplicadas al ingreso de los paquetes.	2048
73	Funcionalidad de 802.1x en cada por puerto.	EXIGIDO
74	Múltiples suplicantes en un mismo puerto físico validándolos en forma independiente.	EXIGIDO
75	Integración con sistemas de control de acceso por medio del protocolo RADIUS y 802.1x para autenticación de usuario.	EXIGIDO
76	El estándar 802.1X está basado en EAP (Extensible Authentication Protocol). Los switches deberán soportar los siguientes métodos de EAP:	EXIGIDO
77	EAP-MD5	EXIGIDO
78	EAP-TLS	EXIGIDO
79	EAP-TTLS	OPCIONAL
80	EAP-PEAP	EXIGIDO
81	Una vez que los dispositivos son autenticados podrán recibir parámetros, vía atributo de RADIUS, de las Listas de Acceso correspondientes.	EXIGIDO
82	Autenticación por dirección MAC sobre un servidor Radius.	EXIGIDO
83	Asignar VLAN cuando la autenticación fue realizada por Dirección MAC	EXIGIDO
84	Autenticación mediante portal cautivo	EXIGIDO
	FUNCIONES DE ALTA DISPONIBILIDAD	
85	Deberá soportar la agregación de interfaces para formar un único link, esta técnica es conocida como LAG (Link Aggregation Group) bajo la norma 802.3ad	EXIGIDO
86	Cantidad mínima de grupos LAG por sistema	≥ 126
87	Cantidad mínima de puertos pertenecientes a grupos LAG	≥ 16
88	Soporte de LACP - Link Aggregation Control Protocol	EXIGIDO
89	Mecanismo de protección contra loops de L2: 802.1D (Spanning Tree), 802.1w (Rapid Spanning Tree) y 802.1s (Multiple Spanning Tree)	EXIGIDO
	ADMINISTRACION	
90	Configuración por línea de comandos vía Telnet, SSHv2 y Serial	EXIGIDO
91	Configuración vía https	EXIGIDO
92	Monitoreo remoto mediante SNMP v1, v2 y v3	v2c, v3
93	Autenticación de usuarios de administración.	Local, RADIUS y TACACS+
94	No debe almacenar el password de los administradores localmente , se debe generar un hash MD5 o SHA1 en configuración local	EXIGIDO
95	Cantidad mínima de configuraciones anteriores a almacenar automáticamente con fines de auditoría	25
96	Soporte configuración de rescate almacenada especialmente por el administrador	EXIGIDO
97	Permitirá deshacer cambios de configuración que no se confirmen dentro de un plazo prestablecido	EXIGIDO
98	Permitirá la configuración de funciones de RMON (RFC 2819)	EXIGIDO
99	Soporte de sFlow con sampling/muestreo sobre tráfico entrante y saliente	EXIGIDO

100	Capacidad de Soportar la función de envío de pruebas para evaluar el desempeño en tiempo real de la red (RPM)	EXIGIDO
	NORMAS Y ESTANDARES	
101	RFC 1122 Host Requirements	EXIGIDO
102	RFC 768 UDP	EXIGIDO
103	RFC 791 IP	EXIGIDO
104	RFC 783 TFTP	EXIGIDO
105	RFC 792 ICMP	EXIGIDO
106	RFC 793 TCP	EXIGIDO
107	RFC 826 ARP	EXIGIDO
108	RFC 894 IP over Ethernet	EXIGIDO
109	RFC 903 RARP	EXIGIDO
110	RFC 906 TFTP Bootstrap	EXIGIDO
111	RFC 1027 Proxy ARP	EXIGIDO
112	RFC 2068 HTTP server	EXIGIDO
113	RFC 1812 Requirements for IP Version 4 Routers	EXIGIDO
114	RFC 1519 CIDR	EXIGIDO
115	RFC 1256 IPv4 ICMP Router Discovery (IRDP)	EXIGIDO
116	RFC 1587 OSPF NSSA Option	EXIGIDO
117	RFC 1058 RIP v1	EXIGIDO
118	RFC 2453 RIP v2	EXIGIDO
119	RFC 1492 TACACS+	EXIGIDO
120	RFC 2138 RADIUS Authentication	EXIGIDO
121	RFC 2139 RADIUS Accounting	EXIGIDO
122	RFC 3579 RADIUS EAP support for 802.1x	EXIGIDO
123	RFC 2080 RIPng for IPv6	EXIGIDO
124	RFC 2154 OSPF w/Digital Signatures (password, MD-5)	EXIGIDO
125	RFC 5176 Dynamic Authorization Extensions to RADIUS	EXIGIDO
126	RFC 2030 SNTP, Simple Network Time Protocol	EXIGIDO
127	RFC 854 Telnet client and server	EXIGIDO
128	RFC 951, 1542 BootP	EXIGIDO
129	RFC 2338 VRRP	EXIGIDO
130	RFC 2131 BOOTP/DHCP relay agent and DHCP server	EXIGIDO
131	RFC 1591 DNS	EXIGIDO
132	RFC 2474 DiffServ Precedence	EXIGIDO
133	RFC 2598 DiffServ Expedited Forwarding (EF)	EXIGIDO
134	RFC 1981 Path MTU Discovery for IPv6	EXIGIDO
135	RFC 4915 MT-OSPF	EXIGIDO
136	RFC 2328 OSPF v2 (edge-mode)	EXIGIDO
137	RFC 2267 Network Ingress Filtering	EXIGIDO
138	RFC 2597 DiffServ Assured Forwarding (AF)	EXIGIDO
139	RFC 5643 OSPF v3 MIB support	EXIGIDO
	ALIMENTACION ELECTRICA, VENTILACION Y DIMENSIONES	
140	Tensión de operación Fuente de Alimentación	100-120V / 200-240V auto detectable.
141	Fuente de alimentación redundante soportado e incluido	EXIGIDO

142	Fuente de alimentación remplazable en caliente	EXIGIDO
143	Ventiladores redundantes	EXIGIDO
144	Ventiladores remplazables en caliente	EXIGIDO
145	Montaje en rack de 19”	EXIGIDO
	Alimentación Eléctrica, Ventilación y dimensiones.	
146	Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	EXIGIDO
147	Cumplimiento de ROHS, EMC certification, Safety certification, Manufacturing certification	OPCIONAL
148	Temperatura de operación: 0°C a 45°C	EXIGIDO
149	Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	EXIGIDO
150	Montaje en rack de 19”	EXIGIDO
151	Cantidad de Unidad de Rack del Equipo	1U

ITEM 2 - SWITCHES DE DATA CENTER

Nro	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	3 (tres)
5	Descripcion	Switch de Datacenter
6	Tipo de uso	Data Center
	Rendimiento y capacidad	
7	Capacidad mínima de forwarding soportado por equipo	≥ 490Mpps
8	Capacidad mínima de conmutación soportada por equipo	≥ 800 Gbps
9	Capacidad mínima de forwarding entre módulos o miembros del stacking (backplane) soportado por equipo	≥ 300 Gbps
10	El equipo deberá estar equipado con la cantidad de Memoria RAM y FLASH mínima necesaria para soportar todas las funcionalidades de la última versión del sistema operativo en el momento de la entrega del equipo y los requerimientos de prestaciones y performance solicitadas en estas especificaciones técnicas.	RAM/ DRAM ≥ 4GB
11	MTBF Mínimo Requerido	≥ 87.600 Hs.
	Interfaces	
12	Cantidad mínima de interfaces ópticas Gigabit Ethernet independientes instalados	≥ 36
13	Cantidad mínima de interfaces 40/100GbE QSFP28 independientes instalados	≥ 2
14	Cantidad mínima de interfaces de 10 GbE ópticas instaladas (independientes de los items anteriores)	≥ 12
15	Capacidad de crecimiento mínima en interfaces de 10GbE y/o 25GbE	≥ 4
16	Cantidad mínima de puertos seriales independientes para administración fuera de banda del equipo.	≥ 1
17	Cantidad mínima de puertos RJ-45 para ser usado como consola de administración.	≥ 1
18	Modulos SFP+ FO (a incluir) para velocidades 10Gbps	24 en total (8 por equipo)
19	Modulos SFP a Cobre (a incluir) para velocidades 10Gbps	18 en total (6 por equipo)

20	Modulos SFP a Cobre (a incluir) para velocidades 1Gbps	72 en total (24 por equipo)
21	Patchcord FO (a incluir)	24 en total (8 por equipo)
	Stacking/Apilamiento	
22	Vinculación de equipos por puertos con interfaces que soporten mínimo 40GbE	EXIGIDO
23	Configuración desde una única dirección IP y para su administración actuarán como un único equipo.	EXIGIDO
24	El reemplazo de un miembro del stack deberá ser no disruptivo. En caso que la versión de Sistema Operativo del equipo a incorporar sea distinta de la vigente el stack/Virtual Chasis , la misma deberá poder actualizarse automáticamente desde el equipo controlador del stack/Master del Virtual Chasis	EXIGIDO
25	Capacidad de conformar un único equipo desde el punto de vista de la administración	EXIGIDO
26	Mínimo de equipos agrupados para administrar con un único acceso administrativo	≥ 2
27	Los puertos miembros de un grupo de Link Aggregation (802.3ad) LAG deben poder pertenecer a diferentes miembros del Stack	EXIGIDO
	FUNCIONES SWITCH DE RED	
28	Todas las interfaces se podrán utilizar independientemente en modo L3 o L2 , es decir se podrán agrupar para formar un dominio de Broadcast (L2) representadas por una interfase L3 virtual (Interfase VLAN) o cada interfase física o lógica podrá configurarse con una dirección IP independiente (L3)	EXIGIDO
29	Funcionalidad de Servidor DHCP	EXIGIDO
30	Funcionalidad de Cliente DHCP	EXIGIDO
31	Funcionalidad de DHCP Relay y Helper	EXIGIDO
32	Protocolo de enrutamiento RIPv1, RIPv2	EXIGIDO
33	Capacidad de soporte para Protocolo de enrutamiento OSPF v2, v3	EXIGIDO
34	Soporte de Bidirectional Forwarding Detection (BFD) con instalacion futura de licencia correspondiente	EXIGIDO
35	Soporte de protocolo de enrutamiento BGP	EXIGIDO
36	Soporte de protocolo de encapsulamiento VXLAN	EXIGIDO
37	Debe soportar la funcionalidad de ruteo por distintos campos del paquete IP como Origen/Destino o puertos (Policy Based Routing o Filter Based Routing) en forma independiente a la tabla de ruteo por defecto	EXIGIDO
38	Mínimo VLANS soportadas – 802.1q Vlan Tagging	≥ 4000
39	Mínimo de direcciones MAC	≥ 100000
40	Mínimo de rutas IPv4 unicast	≥ 100000
41	Mínimo de rutas multicast IPv4	40000
42	Multiple VLAN Registration Protocol (802.1ak)	EXIGIDO
	MULTICAST	
43	Los switches deberán tener la capacidad de interactuar con tráfico multicast para ello deberán soportar los siguientes protocolos :	EXIGIDO
44	IGMP Snooping	EXIGIDO
45	Capacidad de Soporte de IGMP v1 v2 y v3	EXIGIDO
46	Soporte PIM (Protocol Independant Multicast) en modo Sparse, SSM y DM	EXIGIDO
47	Capacidad de Soporte de protocolo MSDP (Multicast Source Discovery Protocol)	EXIGIDO
	ENRUTAMIENTO	

48	RIP v1 y v2	EXIGIDO
49	OSPF v2 y v3	EXIGIDO
50	BGP	EXIGIDO
51	VXLAN	EXIGIDO
	Management	
52	Syslog, Telnet, SSH	EXIGIDO
53	Neighbor DiscoveryProtocol	EXIGIDO
54	IPv6 ping	EXIGIDO
55	MLDv1 v2	EXIGIDO
	CALIDAD DE SERVICIO	
56	Mínimo de colas por hardware de calidad de servicio por interfase	10
57	Configuración por políticas de Calidad de Servicio asociando y marcando el tráfico a una determinada Clase de Servicio:	EXIGIDO
58	por Interfase	EXIGIDO
59	por dirección MAC	EXIGIDO
60	por campo 802.1p	EXIGIDO
61	por VLAN	EXIGIDO
62	por dirección IP origen y/o Destino	EXIGIDO
63	por campo DSCP/IP precedente	EXIGIDO
64	por puertos TCP/UDP	EXIGIDO
65	Configurar la Priorización del tráfico Saliente para cada clase de Servicio	EXIGIDO
	SEGURIDAD	
66	Limitar la cantidad de Direcciones MAC por puerto.	EXIGIDO
67	Deberá soportar MACSEC	EXIGIDO
68	Dynamic ARP inspection (DAI)	EXIGIDO
69	Deberá soportar Local Proxy ARP	EXIGIDO
70	Debera soportar Proxy ARP por VLAN	EXIGIDO
71	Deberá soportar DHCP Snooping	EXIGIDO
72	Deberá soportar Static ARP	EXIGIDO
	CONTROL DE ACCESO Y AUTENTICACION	
73	Cantidad mínima de ACL basadas en el puerto aplicadas al ingreso de los paquetes.	2048
74	Cantidad mínima de ACL basadas en el VLAN aplicadas al ingreso de los paquetes.	2048
75	Funcionalidad de 802.1x en cada por puerto.	EXIGIDO
76	Múltiples suplicantes en un mismo puerto físico validándolos en forma independiente.	EXIGIDO
77	Integración con sistemas de control de acceso por medio del protocolo RADIUS y 802.1x para autenticación de usuario.	EXIGIDO
78	El estándar 802.1X está basado en EAP (Extensible Authentication Protocol). Los switches deberán soportar los siguientes métodos de EAP:	EXIGIDO
79	EAP-MD5	EXIGIDO
80	EAP-TLS	EXIGIDO
81	EAP-TTLS	OPCIONAL
82	EAP-PEAP	EXIGIDO

83	Una vez que los dispositivos son autenticados podrán recibir parámetros, vía atributo de RADIUS, de las Listas de Acceso correspondientes.	EXIGIDO
84	Autenticación por dirección MAC sobre un servidor Radius.	EXIGIDO
85	Asignar VLAN cuando la autenticación fue realizada por Dirección MAC	EXIGIDO
86	Autenticación mediante portal cautivo	EXIGIDO
	FUNCIONES DE ALTA DISPONIBILIDAD	
87	Deberá soportar la agregación de interfaces para formar un único link, esta técnica es conocida como LAG (Link Aggregation Group) bajo la norma 802.3ad	EXIGIDO
88	Cantidad mínima de grupos LAG por sistema	≥ 120
89	Cantidad mínima de puertos pertenecientes a grupos LAG	≥ 10
90	Soporte de LACP - Link Aggregation Control Protocol	EXIGIDO
91	Mecanismo de protección contra loops de L2: 802.1D (Spanning Tree), 802.1w (Rapid Spanning Tree) y 802.1s (Multiple Spanning Tree)	EXIGIDO
	ADMINISTRACION	
92	Configuración por línea de comandos vía Telnet, SSHv2 y Serial	EXIGIDO
93	Configuración vía https	EXIGIDO
94	Monitoreo remoto mediante SNMP v1, v2 y v3	v2c, v3
95	Autenticación de usuarios de administración	Local, RADIUS y TACACS+
96	No debe almacenar el password de los administradores localmente , se debe generar un hash MD5 o SHA1 en configuración local	EXIGIDO
97	Cantidad mínima de configuraciones anteriores a almacenar automáticamente con fines de auditoría	10
98	Soporte configuración de rescate almacenada especialmente por el administrador	EXIGIDO
99	Permitirá deshacer cambios de configuración que no se confirmen dentro de un plazo prestablecido	EXIGIDO
100	Permitirá la configuración de funciones de RMON (RFC 2819)	EXIGIDO
101	Soporte de sFlow con sampling/muestreo sobre tráfico entrante y saliente	EXIGIDO
102	Capacidad de Soportar la función de envío de pruebas para evaluar el desempeño en tiempo real de la red (RPM)	EXIGIDO
	NORMAS Y ESTANDARES	
103	RFC 1122 Host Requirements	EXIGIDO
104	RFC 768 UDP	EXIGIDO
105	RFC 791 IP	EXIGIDO
106	RFC 783 TFTP	EXIGIDO
107	RFC 792 ICMP	EXIGIDO
108	RFC 793 TCP	EXIGIDO
109	RFC 826 ARP	EXIGIDO
110	RFC 894 IP over Ethernet	EXIGIDO
111	RFC 903 RARP	EXIGIDO
112	RFC 906 TFTP Bootstrap	EXIGIDO
113	RFC 1027 Proxy ARP	EXIGIDO
114	RFC 2068 HTTP server	EXIGIDO
115	RFC 1812 Requirements for IP Version 4 Routers	EXIGIDO
116	RFC 1519 CIDR	EXIGIDO

117	RFC 1256 IPv4 ICMP Router Discovery (IRDP)	EXIGIDO
118	RFC 1587 OSPF NSSA Option	EXIGIDO
119	RFC 1058 RIP v1	EXIGIDO
120	RFC 2453 RIP v2	EXIGIDO
121	RFC 1492 TACACS+	EXIGIDO
122	RFC 2138 RADIUS Authentication	EXIGIDO
123	RFC 2139 RADIUS Accounting	EXIGIDO
124	RFC 3579 RADIUS EAP support for 802.1x	EXIGIDO
125	RFC 2080 RIPng for IPv6	EXIGIDO
126	RFC 2154 OSPF w/Digital Signatures (password, MD-5)	EXIGIDO
127	RFC 5176 Dynamic Authorization Extensions to RADIUS	EXIGIDO
128	RFC 2030 SNTP, Simple Network Time Protocol	EXIGIDO
129	RFC 854 Telnet client and server	EXIGIDO
130	RFC 951, 1542 BootP	EXIGIDO
131	RFC 2338 VRRP	EXIGIDO
132	RFC 2131 BOOTP/DHCP relay agent and DHCP server	EXIGIDO
133	RFC 1591 DNS	EXIGIDO
134	RFC 2474 DiffServ Precedence	EXIGIDO
135	RFC 2598 DiffServ Expedited Forwarding (EF)	EXIGIDO
136	RFC 1981 Path MTU Discovery for IPv6	EXIGIDO
137	RFC 4915 MT-OSPF	EXIGIDO
138	RFC 2328 OSPF v2 (edge-mode)	EXIGIDO
139	RFC 2267 Network Ingress Filtering	EXIGIDO
140	RFC 2597 DiffServ Assured Forwarding (AF)	EXIGIDO
141	RFC 5643 OSPF v3 MIB support	EXIGIDO
	ALIMENTACION ELECTRICA, VENTILACION Y DIMENSIONES	
142	Tensión de operación Fuente de Alimentación	100-120V / 200-240V auto detectable.
143	Fuente de alimentación redundante soportado e incluido	EXIGIDO
144	Fuente de alimentación remplazable en caliente	EXIGIDO
145	Ventiladores redundantes	EXIGIDO
146	Ventiladores remplazables en caliente	EXIGIDO
147	Montaje en rack de 19”	EXIGIDO
	Alimentación Eléctrica, Ventilación y dimensiones.	
148	Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	EXIGIDO
149	Cumplimiento de ROHS, EMC certification, Safety certification, Manufacturing certification	OPCIONAL
150	Temperatura de operación: 0°C a 45°C	EXIGIDO
151	Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	EXIGIDO
152	Montaje en rack de 19”	EXIGIDO
153	Cantidad de Unidad de Rack del Equipo	1U

ITEM 3 - SWITCHES DE ACCESO		
Nro.	**Descripción**	**Requerimiento mínimo exigido**

1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	20 (veinte)
5	Capacidad PoE y Power Budget	De los 20 (veinte) equipos solicidados, se requiere 5 (cinco) con capadidad PoE en sus 48 puertos con 750 watts de Power Budget
6	Descripcion	Switch de Acceso de 48 puertos
7	Tipo de configuracion de puertos	Fijos
8	Tipo de uso	Acceso a la Red
	Interfaces y rendimiento	
9	Interfaces independientes 10/100/1000BaseT-Cobre UTP RJ45	48 puertos RJ45
10	Interfaces SFP+ independientes (1/10Gbps)	4 puertos SFP+
11	Puerto 10/100 BaseT Ethernet adicional e independiente para administración del equipo (Out of Band Management)	1 puerto RJ45
12	Puerto SERIAL RS-232 para ser usado como consola de administración	Opcional
13	Puerto USB para el almacenado y descarga de configuraciones y sistema operativo	1 puerto USB
14	Throughput (Maximum with 64 Byte Packets)	130 Mpps
15	Capacidad de conmutacion por paquetes (unidirecional)	85 Gbps
16	Capacidad de conmutacion por paquetes (bidirecional)	170 Gbps
17	Modulos SFP+ FO (a incluir) para velocidades 10Gbps	60 en total (3 por equipo)
18	Patchcord FO (a incluir)	40 en total (2 por equipo)
	Stacking/Apilamiento	
19	Capacidad de backplane del Stack utilizando los puertos de UPLINK	80 Gbps
20	Equipos agrupados para administrar con un único acceso administrativo (mínimo)	≥ 2
21	Deberá soportar el protocolo Link Aggregation Control Protocol (LACP) IEEE 802.3ad.	Exigido
22	Numero de grupos a soportar por todo el STACK (mínimo)	128
	Calidad de Servicio	
23	Encolamiento basado en clases de servicio con priorización de trafico – Strick priority en egreso	Exigido
24	Soporte de Port Shaping : puede ser usados para manjar el excesso de trafico, esta caracteristica define el ancho de banda maximo alojado en un puerto	Exigido
25	Soporte de queuing shaping: puede ser usados para manejar el exceso de trafico, esta caracteristica define el ancho de banda maximo alojado en cada cola	Exigido
26	Soporte de QoS en puertos LAG	Exigido
27	L2 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 2.	Exigido
28	L3 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 3	Exigido
29	Sopoorte de QoS – Clasificacion , re-write y queueing en interfaces RVI (Interface VLANs)	Exigido
30	Soporta el tratamiento de las colas ante congestión con los mecanismos SDWRR (Shaped Deficit Weighted Round Robin) y SPQ (Strict Priority).	Exigido

31	Soporta el protocolo LLDP (Link Layer Discovery Protocol) IEEE 802.1AB y LLDP-MED (LLDP for Media Endpoint Device) ANSI/TIA-1057 integrado para Voice sobre IP (VoIP)	Exigido
32	Soporte de priorización de tráfico de salida por hardware mínimo ocho (8) colas de servicio por puerto.	Exigido
33	Politicas de trafico de red que limitan la velocidad de entrada y salida de una clase de trafico con base en el criterio establecido por el usuario. Permite control la velocidad maxima de trafico enviado o recibido en una interfaz y particionar una red en multiples nieles de clase de servicio	Exigido
34	Encolado estricto y de baja latencia (Strict priority queuing or Low Latency Queuing (LLQ)Strict priority queuing, or low latency queuing (LLQ): es una caracteristica usada para reeenviar de forma mas rapida ciertos tipos de trafico sensible a retardos (voz, video etc)	Exigido
35	Trust 802.1p/DSCP/IP Prec (ingress)	Exigido
36	Soporte de limitación de tráfico mediante lista de control de acceso (ACL) aplicable en los puertos fisicos o VLANs por:	
37	Filtros basados en direcciones MAC origen o destino	Exigido
38	Filtros basados en direcciones IP origen o destino	Exigido
39	Filtros basados en número de puerto TCP/UDP	Exigido
40	Cantidad de filtros de trafico (ACL) (mínimo)	1500
	Spanning Tree Protocol	
41	IEEE 802.1d.	Exigido
42	Rapid Spanning Tree IEEE 802.1w	Exigido
43	Multiple Spanning Tree Protocol IEEE 802.1s.	Exigido
	Soporte de ruteo layer 3 por medio de los siguientes protocolos :	
44	Rutas Estáticas	Exigido
45	Soporte maximo de rutas IPv4	512 prefijos ; 4096 rutas
46	Soporte de IEEE802.1ag Ethernet OAM connectivity fault management (CFM)	Exigido
47	Soporte de Ethernet ring protection switching (ERPS, G.8032/Y.1344)	Exigido
48	Soporte de TDR (Time Domain Reflectometry). Una tecnologia que permite el segumiento y senializacion de fallas en los cables o conectores de redes de computadoras. Los puertos deben ser capaces de generar un pulso electromagnético, cuando este pulso alcanza un obstáculo o el fin del cable se genera un eco que es traducido en la distancia a la falla .	Opcional
49	RIP v1/v2	Exigido
50	RIPng	Exigido
51	Soporte OSPF	Exigido
52	Soporte de Layer 2 protocol tunneling (L2PT)	Exigido
53	Soporte de ARP (numero de entradas)	1024
	Funcionalidades layer 2	
54	Soporte de direcciones MAC de red (mínimo)	15000
55	Soporte de tramas Jumbo	Exigido
56	Soporte de IEEE 802.1X para VLAN VoIP.	Exigido
57	Port-based VLAN	Exigido
58	MAC-based VLAN	Exigido
59	Soporte IEEE 802.1Q-in-Q: VLAN Stacking	Exigido

60	IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)	Exigido
61	Compatible con Per-VLAN Spanning Tree Plus	Exigido
62	Soporte de interfaces RVI (Routed VLAN Interfaces)	Exigido
63	Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en todos los puertos según IEEE 802.1 p/Q.	Exigido
64	Numero de VLANs configurables en el Virtual Chasis (mínimo)	4000
65	VLANS en equipo individual (mínimo)	4000
66	Posible rango de VLAN-ID para configurar	Entre 1 - 4000
67	Soporte de DHCP Relay y DHCP helper	Exigido
68	Soporte de DHCP Server sobre interfaces RVI	Exigido
69	Voice VLAN fallback	Exigido
	Multicast	
70	Soporte protocolo IGMP-Snooping	Exigido
71	Soporte PIM-SM, PIM-SSM, PIM-DM	Exigido
72	Soporte IGMP: v1, v2, v3	Exigido
	Administracion / Management	
73	Deberá soportar Simple Network Management Protocol versión SNMP v2c ,SNMP v3.	Exigido
74	Capacidad de proveer los bloques de información de management (MIBs) necesarios.	Exigido
75	Capacidad de Remote Monitoring (RMON), deberá soportar al menos cuatro (4) grupos (statistics, history, alarm, events).	Exigido
76	sFlow	Exigido
77	Soporte de registro remoto (SysLog).	Exigido
78	Soporte de traffic mirroring por puerto o por VLAN.	Exigido
79	Deberá soportar Network Timing Protocol (NTP).	Exigido
80	Creación de perfiles de administrador con facultadas especificas de modificar la configuración o solo acceder a vistas de la misma y listado de comandos disponibles para ejecutar por cada perfil	Exigido
81	Las passwords (claves) de administrador almacenadas localmente deben estar encriptadas usando hash MD5 o SHA1	Exigido
82	Soporte de MIB para la información de media attachment unit (MAU)	Exigido
83	Fuente para AC	Exigido
84	Accesorios necesarios para montar en racks estándar de 19”.	Exigido
	Seguridad, mecanismos soportados	
85	Central Web authentication	Exigido
86	Deberá soportar autentificación 802.1X. para diferentes VLANs por puerto.	Exigido
87	Soporte de IEEE 802.1X con soporte de VLANs de invitados (Guest VLAN)	Exigido
88	MAC Radius Authentication con 802.1X	Exigido
89	Soporte de protocolo EAP-PAP para MAC RADIUS authentication	Exigido
90	Soporte de seguridad del puerto mediante filtrado por dirección MAC. En caso de violación del puerto deberá poder enviarse una alerta al administrador y deshabilitar el puerto.	Exigido
91	Soporte de limitación de direcciones MAC por puerto.	Exigido
92	Soporte de Persistent MAC learning o sticky MAC	Exigido
93	DHCP Snooping.	Exigido

94	Dynamic ARP inspection (DAI)	Exigido
95	Proxy ARP	Exigido
96	Static ARP support	Exigido
97	IP source guard	Exigido
98	Orden de autenticación flexible	Exigido
99	IPv6 Neighbor Discovery inspection	Exigido
	Servicio de configuración por medios seguros	
100	Soporte Telnet / Secure Shell (SSH) versión 2 para conexión remota vía interfaz línea de comando (CLI).	Exigido
101	Soporte vía Web con SSL. (HTTPS)	Exigido
102	Soporte de creación de Certificados locales para conexión HTTPs	Exigido
103	Almacenamiento de sistema operativo y configuración en memoria Flash reescribible. (mínimo)	1 GB
104	Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	Exigido
105	Mecanismos de automatización mediante scripts o similares que permitan chequear el cumplimiento y administrar los cambios de configuraciones, aplicar configuraciones predefinidas, visualizar conjuntos de comandos para el diagnóstico, análisis y administración de eventos, y generar respuestas predefinidas a eventos.	Exigido
106	Configuración por medio de consola serial asincrónica. Proveer al menos cinco cables	Exigido
107	La unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados como original en papel ó en CD-ROM.	Exigido
108	Equipos alimentados con 220 V - 50 Hz, monofásico con toma de 3 patas, sin necesidad de requerir un transformador adicional.	Exigido
	Troubleshooting	
109	Debugging: CLI via console, telnet, or SSH	Exigido
110	Diagnostics: Show and debug command statistics	Exigido
111	Traffic mirroring (port)	Exigido
112	Traffic mirroring (VLAN)	Exigido
113	ACL-based mirroring	Exigido
114	Mirroring destination ports per system	Exigido
115	LAG port monitoring	Exigido
116	Multiple destination ports monitored to 1 mirror (N:1)	Exigido
117	Maximum number of mirroring sessions	Exigido
118	Mirroring to remote destination (over L2)	Exigido
119	IP tools: Extended ping and trace	Exigido
	Alta disponibilidad	
120	Soporte de Link Aggregation	Exigido
121	802.3ad (LACP) support: Number of LAGs supported	128
122	Maximum number of ports per LAG:	8
	LAG sharing algorithm—Routed Multicast Traffic:	
123	Tagged ports support in LAG	Exigido
124	Uplink Failure Detection (UFD)	Exigido

125	Soporte para equipos con dos Routing engines, configurar al Routing engine de respaldo para asumir el rol de master sin causar interrupcion en el reenvio.	Exigido
126	Soporte VRRP (Virtual Router Redundancy Protocol)	Exigido
	Alimentación Eléctrica, Ventilación y dimensiones.	
127	Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	Exigido
128	Cumplimiento de ROHS, EMC certification, Safety certification, Manufacturing certification	Opcional
129	Temperatura de operación: 0°C a 45°C	Exigido
130	Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	Exigido
131	Montaje en rack de 19”	Exigido
132	Cantidad de Unidad de Rack del Equipo	1U
133	MTBF (mínimo)	87.600 hs

LOTE N° 2 – ADQUISICIÓN DE EQUIPOS DE SEGURIDAD FORTINET

ITEM N° 1 - SOLUCIÓN ANTISPAM Y SEGURIDAD PARA CORREO

Nro.	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	2 (dos)
	Requisitos Mínimos	**REQUERIDO**
5	Mínimo 4 interfaces RJ45 10/100/1000	REQUERIDO
6	Se deben poder configurar al menos 60 dominios de correo electrónico en la solución	REQUERIDO
7	La solución debe incluir al menos dos discos de 1 TB y debe soportar arreglos RAID 0 y RAID 1 mínimamente por software	REQUERIDO
8	La solución debe poder también tener la capacidad de ser configurada como servidor de correo electrónico, soportando un mínimo de 380 casillas de correo.	REQUERIDO
9	La solución debe soportar la configuración de al menos 200 políticas de remitentes por cada dominio.	REQUERIDO
10	La solución debe ser capaz de procesar un mínimo de 240.000 mensajes de correo electrónico por hora.	REQUERIDO
11	La solución debe ser capaz de procesar un mínimo de 180.000 mensajes de correo electrónico por hora con la funcionalidad de Anti-Spam activada.	REQUERIDO
12	La solución debe ser aprovisionada en formato de appliance físico.	REQUERIDO
	Implementación y Modos de Operación	**REQUERIDO**
13	Todas las funcionalidades deben ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo y por un periodo mínimo de 36 meses.	REQUERIDO

14	Solución debe basarse en "appliance" de proposito especifico (Fisico). No se tendrán en cuenta los equipos de uso general (PCs o servidores) en la que se puede instalar y / o ejecutar un sistema operativo regular, como Microsoft Windows, FreeBSD, Solaris de Sun o GNU / Linux.	REQUERIDO
15	La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.	REQUERIDO
16	La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent).	REQUERIDO
17	La solución debe ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidas.	REQUERIDO
18	Debe poder ser instalado en forma de proxy SMTP transparente, para el análisis de correo saliente, buscando evitar el reporte en Blacklist	REQUERIDO
19	La solución debe soportar su implementación en modo de servidor, operando como un servidor de correo MTA independiente con buzones para los usuarios. Debe ser capaz de almacenar localmente mensajes de correo electrónico para su entrega a los usuarios a través de correo Web, POP3 y / o IMAP.	REQUERIDO
20	Debe tener disponible un API basado en REST para fines de monitoreo, automatización y orquestación.	REQUERIDO
21	La solución debe ser licenciada sin importar el número de buzones que proteja. El licenciamiento es basado en el performance del hardware suministrado (correo por hora)	REQUERIDO
	Características Generales de Seguridad de Correo Electrónico	**REQUERIDO**
23	La solución debe soportar listas blancas (seguras) y negras por dirección de correo, por dominio y direcciones IP	REQUERIDO
24	La solución debe permitir la sobreescritura, la edición y personalización de los mensajes de notificación de antivirus.	REQUERIDO
25	La solución debe poder permitir aplicar políticas basadas en la dirección IP del remitente	REQUERIDO
26	La solución debe proporcionar soporte para múltiples dominios de correo electrónico.	REQUERIDO

27	La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente.	REQUERIDO
28	La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.	REQUERIDO
29	La solución debe soportar cuarentena por usuario, permitiendo que cada usuario puede gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo.	REQUERIDO
30	La solución debe ser capaz de programar el envío de informes de cuarentena.	REQUERIDO
31	La solución debe ser capaz de realizar el almacenamiento (o archivado) de correo electrónico, basado en políticas, por ejemplo, archivado de correos electrónicos basado en ciertos remitentes o si el correo electrónico contiene determinadas palabras.	REQUERIDO
32	La solución debe ser capaz de mantener la cola de correo en caso de fallo en la conexión de salida, retrasos o errores de entrega.	REQUERIDO
33	La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP.	REQUERIDO
34	La solución debe ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados.	REQUERIDO
35	La solución debe ser compatible con el enrutamiento en IPv4 y IPv6.	REQUERIDO
36	La solución debe permitir el almacenamiento de correo electrónico a nivel local o servidor remoto.	REQUERIDO
37	La solución debe tener características antispam y antivirus	REQUERIDO
38	La solución debe ser capaz de realizar la inspección del correo de Internet entrante y saliente.	REQUERIDO

39	La solución debe contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger	REQUERIDO
40	La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb	REQUERIDO
41	La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing.	REQUERIDO
	Funcionalidades de Anti-Spam	**REQUERIDO**
42	La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam.	REQUERIDO
43	La solución puede detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante.	REQUERIDO
44	La solución debe contar con mecanismos de detección de SPAM nuevo, mediante el análisis continuo de los correo recibidos y su posterior correlación con eventos ocurridos a nivel mundial, permitiendo así definir y detectar nuevas reglas de SPAM	REQUERIDO
45	La solución debe ser capaz de realizar análisis Heurístico y definir umbrales máximos de acuerdo al comportamiento del correo y así determinar si un correo es spam.	REQUERIDO
46	La solución debe ser capaz de realizar análisis Bayesiano para determinar si un correo es spam.	REQUERIDO
47	La solución debe ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter).	REQUERIDO
48	La solución debe contar con técnica que detecten SPAM mediante el uso de Greylist, las cuales clasifican el correo con base en su compartimiento en el inicio de sesión, como bloquear todos los correos y permitir solo los reenvíos.	REQUERIDO
49	La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words).	REQUERIDO
50	La solución debe contar con Diccionarios predefinidos de palabras que pueden ser escaneados en el correo electrónico, además definir pesos a cada diccionario o palabra creada para definir si un correo es SPAM.	REQUERIDO

51	La solución permite crear lista blancas o negras de palabras.	REQUERIDO
52	La solución debe permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal, sobre escribir el destinatario, Archivar, enviar copia oculta BCC, reenviar a otro Host, Insertar un TAG o un nuevo encabezado.	REQUERIDO
53	La solución debe ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM.	REQUERIDO
54	La solución debe ser capaz de soportar las listas negras de terceros tales como DNSBL y SURBL.	REQUERIDO
55	La solución permite identificar imágenes que hagan alusión a contenido SPAM. Debe soportar el análisis (al menos) de las siguientes extensiones GIF, JPEG, PNG.	REQUERIDO
	Manejo de Sesiones	**REQUERIDO**
56	La solución debe ser compatible con Sender Policy Framework (SPF).	REQUERIDO
57	La solución debe ser compatible con Domain Keys Identified Mail (DKIM).	REQUERIDO
58	La solución debe ser compatible con Domain Based Message Authentication (DMARC).	REQUERIDO
59	La solución debe identificar altos volúmenes de conexiones y aplicar limites basado en senders e Ips.	REQUERIDO
60	La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico.	REQUERIDO
	Administración y Alta Disponibilidad (HA)	**REQUERIDO**
61	La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS).	REQUERIDO
62	La solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.	REQUERIDO

63	La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only)	REQUERIDO
64	La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como anti-spam, anti-virus, autenticación, entre otros.	REQUERIDO
65	La solución debe permitir esquemas de alta disponibilidad, tanto Activo-Activo como Activo-Pasivo	REQUERIDO
66	Cuando la solución se implementa para alta disponibilidad debe ser capaz de controlar el estado del enlace.	REQUERIDO
67	Cuando la solución se implementa para alta disponibilidad, debe ser capaz de sincronizar los mensajes de e-mails en cuarentena.	REQUERIDO
68	Cuando la solución se implementa para alta disponibilidad activo / Pasivo debería ser posible sincronizar los mensajes de correo electrónico y configuraciones.	REQUERIDO
69	Cuando la solución se implementa para alta disponibilidad debe ser capaz de detectar y reportar el fallo de un dispositivo.	REQUERIDO
	Funcionalidades de Protección Anti-Malware	**REQUERIDO**
70	La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail.	REQUERIDO
71	La solución debe ser capaz de ejecutar el análisis antivirus en archivos comprimidos como RAR, ARJ, LHA, ZIP y PKZIP.	REQUERIDO
72	La solución debe contar con una base de datos de malware suministrada por el fabricante, la cual puede ser actualizada recurrentemente.	REQUERIDO
73	Ante la detección de un malware, la solución puede ejecutar las siguientes acciones: reenviar el correo y el malware a una cuenta definida, reescribir el destinatario.	REQUERIDO
74	La solución debe tener la capacidad de realizar protección anti-malware basándose en analíticas de su propia plataforma de inteligencia de amenazas, y por lo tanto, permitir la identificación rápida de nuevas amenazas.	REQUERIDO
	Funcionalidades de DLP	**REQUERIDO**
75	También debe proporcionar una solución DLP para detectar la información sensible que puede estar llegando por e-mail.	REQUERIDO
76	La funcionalidad DLP debe permitir definir la información a detectar como palabras, frases y expresiones regulares.	REQUERIDO

77	La funcionalidad DLP debe tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros.	REQUERIDO
78	La funcionalidad DLP debe permitir la creación y almacenamiento de impresiones digitales (Fingerprint) de documentos.	REQUERIDO
79	La funcionalidad DLP para permitir la creación de filtros por tipos de archivos;	REQUERIDO
80	La funcionalidad DLP debe permitir la generación y almacenamiento de impresiones digitales (fingerprints) de los archivos adjuntos de correo electrónico.	REQUERIDO
81	La funcionalidad DLP debe permitir el almacenamiento de impresiones digitales (Fingerprints) de archivos antiguos y también para los nuevos archivos que se han actualizado.	REQUERIDO
	Encriptacion y Cifrado	**REQUERIDO**
82	Debe soportar cifrado de mensajes basado en identidad (IBE-Identity Based Encryption), de tal forma que el destinatario no requiera de un PSK o certificado previamente instalado para su descifrado	REQUERIDO
83	El cifrado de mensajes con IBE, debe soportar tanto el metodo push como pull, donde el mensaje cifrado estará almacenado en la plataforma de correo para su acceso remoto autenticado, o bien sea enviado como un adjunto al destinatario.	REQUERIDO
84	En ambos métodos de cifrado con IBE se debe contar con un registro del destinatario en la plataforma de correo, de tal forma que para ver los mensajes cifrados se requiera un proceso de autenticación.	REQUERIDO
85	Debe soportar cifrado de correo usando S/MIME	REQUERIDO
86	Debe soportar cifrado SMTPS	REQUERIDO
	Registros y Reportes	**REQUERIDO**
87	La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog).	REQUERIDO
88	La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.	REQUERIDO
89	La solución debe generar informes por demanda o programados a intervalos de tiempo específicos	REQUERIDO
90	La solución debe generar y enviar informes en formato PDF o HTML.	REQUERIDO
	RFCs	**REQUERIDO**
91	Debe soportar el RFC 1213 (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II)	REQUERIDO
92	Debe soportar el RFC 1918 (Address Allocation for Private Internets)	REQUERIDO

93	Debe soportar el RFC 1985 (SMTP Service Extension for Remote Message Queue Starting)	REQUERIDO
94	Debe soportar el RFC 2034 (SMTP Service Extension for Returning Enhanced Error Codes)	REQUERIDO
95	Debe soportar el RFC 2045 (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies)	REQUERIDO
96	Debe soportar el RFC 2505 (Anti-Spam Recommendations for SMTP MTAs)	REQUERIDO
97	Debe soportar el RFC 2634 (Enhanced Security Services for S/MIME)	REQUERIDO
98	Debe soportar el RFC 2920 (SMTP Service Extension for Command Pipelining)	REQUERIDO
99	Debe soportar el RFC 3207 (SMTP Service Extension for Secure SMTP over TLS)	REQUERIDO
100	Debe soportar el RFC 3461 (SMTP Service Extension for Delivery Status Notifications DSNs)	REQUERIDO
101	Debe soportar el RFC 3463 (Enhanced Mail System Status Codes)	REQUERIDO
102	Debe soportar el RFC 3464 (Extensible Message Format for Delivery Status Notifications)	REQUERIDO
103	Debe soportar el RFC 3635 (Definitions of Managed Objects for the Ethernet-like Interface Types)	REQUERIDO
104	Debe soportar el RFC 4954 (SMTP Service Extension for Authentication)	REQUERIDO
105	Debe soportar el RFC 5321 (SMTP)	REQUERIDO
106	Debe soportar el RFC 5322 (Internet Message Format)	REQUERIDO
107	Debe soportar el RFC 6376 (DomainKeys Identified Mail (DKIM) Signatures)	REQUERIDO
108	Debe soportar el RFC 6522 (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages)	REQUERIDO

109	Debe soportar el RFC 6409 (Message Submission)	REQUERIDO
110	Debe soportar el RFC 7208 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail)	REQUERIDO
111	Debe soportar el RFC 2088 (IMAP4 Non-synchronizing Literals)	REQUERIDO
112	Debe soportar el RFC 2177 (IMAP4 Idle Command)	REQUERIDO
113	Debe soportar el RFC 2221 (Login Referrals)	REQUERIDO
114	Debe soportar el RFC 2342 (IMAP4 Namespace)	REQUERIDO
115	Debe soportar el RFC 2683 (IMAP4 Implementation Recommendations)	REQUERIDO
116	Debe soportar el RFC 2971 (IMAP4 ID Extension)	REQUERIDO
117	Debe soportar el RFC 3348 (IMAP4 Child Mailbox Extensión)	REQUERIDO
118	Debe soportar el RFC 3501 (IMAP4 rev1)	REQUERIDO
119	Debe soportar el RFC 3502 (IMAP Multiappend Extensión)	REQUERIDO
120	Debe soportar el RFC 3516 (IMAP4 Binary Content Extensión)	REQUERIDO
121	Debe soportar el RFC 3691 (Unselect Command)	REQUERIDO
122	Debe soportar el RFC 4315 (UIDPLUS Extension)	REQUERIDO
123	Debe soportar el RFC 4469 (Catenate Extension)	REQUERIDO
124	Debe soportar el RFC 4731 (Extension to SEARCH Command for Controlling What Kind of Information Is Returned)	REQUERIDO

125	Debe soportar el RFC 4959 (Extension for Simple Authentication and Security Layer (SASL) Initial Client Response)	REQUERIDO
126	Debe soportar el RFC 5032 (WITHIN Search Extensión)	REQUERIDO
127	Debe soportar el RFC 5161 (Enable Extensión)	REQUERIDO
128	Debe soportar el RFC 5182 (Extension for Referencing the Last SEARCH Result)	REQUERIDO
129	Debe soportar el RFC 5255 (IMAP Internationalization)	REQUERIDO
130	Debe soportar el RFC 5256 (Sort and Thread Extensions)	REQUERIDO
131	Debe soportar el RFC 5258 (List Command Extensions)	REQUERIDO
132	Debe soportar el RFC 5267 (Contexts for IMAP4)	REQUERIDO
133	Debe soportar el RFC 5819 (Extension for Returning STATUS Information in Extended LIST)	REQUERIDO
134	Debe soportar el RFC 6154 (LIST Extension for Special-Use Mailboxes)	REQUERIDO
135	Debe soportar el RFC 6851 (MOVE extensión)	REQUERIDO
136	Debe soportar el RFC 7162 (IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC))	REQUERIDO
137	Debe soportar el RFC 1939 (POP3)	REQUERIDO
138	Debe soportar el RFC 2449 (POP3 Extensión Mechanism)	REQUERIDO
139	Debe soportar el RFC 1155 (Structure and Identification of Management Information for TCP/IP-based Interface)	REQUERIDO
140	Debe soportar el RFC 1157 (SNMP v1)	REQUERIDO

141	Debe soportar el RFC 1213 (MIB 2)	REQUERIDO
142	Debe soportar el RFC 2578 (Structure of Management Information Version 2)	REQUERIDO
143	Debe soportar el RFC 2579 (Textual Conventions for SMIv2)	REQUERIDO
144	Debe soportar el RFC 2595 (Using TLS with IMAP, POP3 and ACAP)	REQUERIDO
145	Debe soportar el RFC 3410 (SNMP v3)	REQUERIDO
146	Debe soportar el RFC 3416 (SNMP v2)	REQUERIDO

ITEM N° 2 - CORTAFUEGOS DE APLICACIONES WEB

Nro.	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	2 (dos)
	Especificaciones de Hardware y Rendimiento	
5	La solución debe de ser del tipo appliance físico	REQUERIDO
6	Throughput (HTTP) minimo de 240 Mbps	REQUERIDO
7	Cantidad de interfaces 1 Gbps (RJ45): mínimo 4	REQUERIDO
8	Cantidad de interfaces 1 Gbps (SFP): mínimo 4	REQUERIDO
9	Cada equipo (appliance físico) debe de tener un firmware específico destinado a la finalidad de Firewall de Aplicación Web (WAF –Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.	REQUERIDO
10	Tener puerto consola RS-232 o RJ45, para acceso a la interfaz de linea de comandos	REQUERIDO
11	Tener LEDs para la indicación del status y actividades de las interfaces	REQUERIDO
12	La solución debe permitir implementación en modo Proxy Transparente, Proxy Reverso y Sniffer	REQUERIDO
13	La solución debe de ser capaz de ser implementada con protocolo WCCP	REQUERIDO
14	Soportar VLANs del estándar IEEE 802.1q.	REQUERIDO
15	Debe de implementar el protocolo Link Aggregation Control Protocol (LACP) - IEEE 802.3ad	REQUERIDO

16	Soportar direccionamiento IPv4 y IPv6 en las interfaces físicas y virtuales (VLANs).	REQUERIDO
17	La solución debe de soportar y brindar cluster de alta disponibilidad entre dos equipos en modo Activo-Pasivo y Activo-Activo, de forma que el tráfico siga siendo procesado en caso de fallo del equipo principal.	REQUERIDO
18	La solución debe de soportar la sincronización de configuración entre dos appliances del mismo tipo, con el objetivo de operar en modo activo-activo, con la distribución de tráfico siendo realizada por balanceador de tráfico externo o por la propia solución.	REQUERIDO
19	La solución debe de soportar enrutamiento por política (policy route)	REQUERIDO
	Administración de la Solución	**REQUERIDO**
20	El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente al equipo por puerto de consola, o remotamente vía SSH.	REQUERIDO
21	Debe de soportar administración basada en interface web	REQUERIDO
22	Tener la función de auto-completar comandos en la CLI	REQUERIDO
23	Tener la función de auto-completar comandos en la CLI	REQUERIDO
24	Tener ayuda contextual en la CLI	REQUERIDO
25	La solución debe de tener un Dashboard con información sobre el sistema (información del cluster, hostname, número de serie, modo de operación, tiempo en servicio, versión de firmware)	REQUERIDO
26	Debe de ser posible visualizar a través de la interfaz gráfica de gestión la información de licencia, firmas y contrato de soporte	REQUERIDO
27	La solución ofertada deberá de tener acceso a la línea de comando CLI directamente a través de la interfaz gráfica de gestión (GUI)	REQUERIDO
28	Debe de proveer, en la interfaz de gestión, la siguiente información del sistema para cada equipo: consumo de CPU y estadísticas de conexión	REQUERIDO
29	Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memoria	REQUERIDO
30	Debe de incluir una herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados	REQUERIDO
31	Debe proveer la siguiente información en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de requisición HTTP en tiempo real y los últimos logs de eventos del sistema	REQUERIDO

32	Tener en la interfaz gráfica estadísticas de conexión concurrente y por segundo, de políticas de seguridad del sistema	REQUERIDO
33	Tener un dashboard de visualización con información de las interfaces de red del sistema	REQUERIDO
34	La configuración de administración de la solución debe permitir la utilización de perfiles	REQUERIDO
35	Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI)	REQUERIDO
36	Debe de tener la opción de cifrar el backup utilizando contraseña	REQUERIDO
37	Debe de ser posible ejecutar y recuperar el backup utilizando FTP	REQUERIDO
38	Debe de ser posible ejecutar y recuperar el backup utilizando SFTP y TFTP	REQUERIDO
39	Debe ser posible probar una nueva versión de firmware en memoria RAM, sin instalar en disco, antes de aplicarla	REQUERIDO
40	Debe ser posible instalar un firmware alternativo en disco y arrancarlo en caso de fallo del firmware principal	REQUERIDO
41	Debe soportar los protocolos de monitoreo SNMP.	REQUERIDO
42	Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog	REQUERIDO
43	La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG	REQUERIDO
44	Debe tener la capacidad de almacenar los logs en appliance remoto	REQUERIDO
45	La solución debe tener datos analíticos conteniendo la localización geográfica de los clientes web	REQUERIDO
46	La solución debe tener datos analíticos, siendo posible visualizar el total de ataques y porcentaje de cada país de origen, el volumen total de tráfico en bytes y porcentaje de cada país de origen, y el total de accesos (hits) y porcentaje de cada país de origen	REQUERIDO
47	Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario	REQUERIDO
48	Debe soportar RESTful API para gestión de la configuración	REQUERIDO
	Autenticación	**REQUERIDO**

49	Los usuarios deben de ser capaces de autenticarse a través del encabezado de autorización HTTP/HTTPS	REQUERIDO
50	Los usuarios deben de ser capaces de autenticarse a través de formularios HTML embebidos	REQUERIDO
51	La solución debe de ser capaz de autenticar los usuarios a través de certificados digitales personales	REQUERIDO
52	Debe tener base local para almacenamiento y autenticación de los usuarios	REQUERIDO
53	La solución debe tener la capacidad de autenticar usuarios en bases externas remotas LDAP, RADIUS y SAML	REQUERIDO
54	La solución debe de ser capaz de autenticar los usuarios en base remota vía NTLM	REQUERIDO
55	La solución debe de ser capaz de crear grupos de usuarios para configurar mecanismos de autenticación por grupos	REQUERIDO
	Regulaciones y Certificaciones	**REQUERIDO**
56	La solución debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP	REQUERIDO
57	El equipo debe de tener certificación FCC Class A part 15	REQUERIDO
58	El equipo debe de tener certificación VCCI	REQUERIDO
59	El equipo debe de tener certificación CE	REQUERIDO
60	El equipo debe de tener certificación UL/CB/cUL	REQUERIDO
	Funcionalidades de Firewall de Aplicaciones Web	**REQUERIDO**
61	Todas las funcionalidades deben ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo y por un periodo mínimo de 36 meses.	REQUERIDO
62	Debe tener soporte nativo de HTTP/2	REQUERIDO
63	Debe soportar traducción de HTTP/2 a HTTP 1.1	REQUERIDO
64	Deberá soportar interoperabilidad con OpenAPI 3.0	REQUERIDO
65	Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica	REQUERIDO
66	La solución debe permitir elegir entre utilizar la base de datos completa o solamente la base de datos que contiene los últimos y más peligrosos virus	REQUERIDO
67	Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no	REQUERIDO

68	Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial	REQUERIDO
69	Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo	REQUERIDO
70	El perfil aprendido de forma automática debe de poder ser ajustado	REQUERIDO
71	Tener la capacidad de creación de firmas personalizadas de ataques	REQUERIDO
72	Tener la capacidad de protección contra ataques del tipo Adobe Flash binary (AMF) protocol.	REQUERIDO
73	Tener la capacidad de protección contra ataques del tipo Botnet	REQUERIDO
74	La solución debe tener funcionalidad de protección contra ataques como acceso por fuerza bruta	REQUERIDO
75	Debe soportar detección de ataques de Clickjacking	REQUERIDO
76	Debe soportar detección de ataques de alteración de cookie	REQUERIDO
77	Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF)	REQUERIDO
78	La solución debe tener funcionalidad de protección contra ataques como cross site scripting (XSS)	REQUERIDO
79	Debe tener protección contra ataques de Denial of Service (DoS);	REQUERIDO
80	Tener la capacidad de protección contra ataques del tipo HTTP header overflow	REQUERIDO
81	Tener la capacidad de protección contra ataques del tipo Local File inclusión (LFI)	REQUERIDO

82	Tener la capacidad de protección contra ataques del tipo Man-in-the-middle (MITM)	REQUERIDO
83	Tener la capacidad de protección contra ataques del tipo Remote File Inclusión (RFI)	REQUERIDO
84	Tener la capacidad de protección contra ataques del tipo Server Information Leakage	REQUERIDO
85	Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection);	REQUERIDO
86	Identificar y prevenir ataques del tipo Low-rate DoS	REQUERIDO
87	Prevención contra Slow POST attack	REQUERIDO
88	Proteger contra ataques Slowloris	REQUERIDO
89	Tener la capacidad de protección contra ataques del tipo SYN flood	REQUERIDO
90	Tener la capacidad de protección contra ataques del tipo Forms Tampering	REQUERIDO
91	La solución debe tener funcionalidad de protección contra ataques de manipulación de campos ocultos	REQUERIDO
92	Tener la capacidad de protección contra ataques del tipo Directory Traversal	REQUERIDO
93	Tener la capacidad de protección del tipo Access Rate Control	REQUERIDO
94	Identificar y proteger contra Zero Day Attacks	REQUERIDO
95	Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold	REQUERIDO
96	Permitir configurar reglas de bloqueo a métodos HTTP no deseados	REQUERIDO
97	Permitir que se configuren reglas de límite de upload por tamaño del archivo	REQUERIDO

98	Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país	REQUERIDO
99	Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado	REQUERIDO
100	Permitir configurar listas de bloqueo y listas de confianza, basadas en dirección IP de origen	REQUERIDO
101	Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataques detectados por la solución	REQUERIDO
102	Debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation	REQUERIDO
103	Tener la capacidad de prevención contra fuga de información (DLP), bloqueando la fuga de información del encabezado HTTP	REQUERIDO
104	Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo	REQUERIDO
105	Tener la funcionalidad de antivírus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo	REQUERIDO
106	Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado	REQUERIDO
107	La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleraración de tráfico	REQUERIDO
108	Para SSL/TLS offload soportar al menos TLS 1.0, 1.1, 1.2 y 1.3	REQUERIDO
109	La solución debe tener la capacidad de almacenar certificados digitales de CA's	REQUERIDO
110	La solución debe de ser capaz de generar CSR para ser firmado por una CA	REQUERIDO

111	La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL	REQUERIDO
112	La solución debe contener las firmas de bots conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones	REQUERIDO
113	La solución debe de tener un sistema de bloqueo con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación debe de ser actualizado automáticamente.	REQUERIDO
114	La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores	REQUERIDO
115	La solución debe permitir la customización o reenvío de request y response HTTP en el Host, URL, Referer, Body y Location	REQUERIDO
116	La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP	REQUERIDO
117	Permitir que se configuren firmas personalizadas de ataques y DLP, a través de expresiones regulares	REQUERIDO
118	La solución debe permitir ejecutar escaneo de vulnerabilidades o la integración con scanners de vulnerabilidades de terceros, tales como Acunetix, IBM AppScan, WhiteHat, entre otros	REQUERIDO
119	Debe permitir programar el escaneo de vulnerabilidades	REQUERIDO
120	La solución debe generar un reporte de análisis de vulnerabilidades y permitir su descarga	REQUERIDO
121	Soportar redirección y reescritura de request y response HTTP	REQUERIDO
122	Permitir redirección de request HTTP hacia HTTPS	REQUERIDO
123	Permitir reescribir la línea URL del encabezado de un request HTTP	REQUERIDO
124	Permitir reescribir el campo HOST del encabezado de un request HTTP	REQUERIDO
125	Permitir reescribir el campo REFERER del encabezado de un request HTTP	REQUERIDO
126	Permitir redirigir request hacia otro website	REQUERIDO
127	Permitir enviar respuesta HTTP 403 Forbidden para request HTTP	REQUERIDO

128	Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección de un servidor web	REQUERIDO
129	Permitir reescribir el cuerpo ("body") de un response HTTP de un servidor web	REQUERIDO
130	Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando se encuentra en modo proxy reverso	REQUERIDO
131	La solución debe de soportar reglas para definir si los request HTTP serán aceptados en función de la URL y origen del request y, si necesario, aplicar una tasa específica de velocidad (rate limit).	REQUERIDO
132	Tener capacidad de caching para acelerar la entrega de contenido web	REQUERIDO
133	Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes	REQUERIDO
	Funcionalidades de Balanceo de Carga	**REQUERIDO**
134	Permitir prueba de disponibilidad del servidor web a través del método HTTP	REQUERIDO
135	Permitir prueba de disponibilidad del servidor web a través del método HTTPS	REQUERIDO
136	En las pruebas de disponibilidad HTTP y HTTPS, permitir indicar la URL exacta a ser probada	REQUERIDO
137	En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir entre los métodos HEAD, GET y POST	REQUERIDO
138	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Host"	REQUERIDO
139	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "URL"	REQUERIDO
140	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Parámetro HTTP"	REQUERIDO
141	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Referer"	REQUERIDO

142	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Dirección IP de Origen"	REQUERIDO
143	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Encabezado".	REQUERIDO
144	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Cookie"	REQUERIDO
145	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Valor del campo del Certificado X509"	REQUERIDO
146	Implementar Cache de Contenido para HTTP, permitiendo que objetos sean almacenados y request HTTP sean contestados directamente por la solución	REQUERIDO
147	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por dirección IP de origen	REQUERIDO
148	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis de cualquier parámetro del header HTTP	REQUERIDO
149	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis del parámetro URL	REQUERIDO
150	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por cookie – método cookie insert y cookie rewrite	REQUERIDO
151	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por embedded cookie (cookie original seguido de porción aleatoria)	REQUERIDO
152	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Reescritura del Cookie	REQUERIDO
153	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Cookie Persistente	REQUERIDO

154	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en ASP Session ID	REQUERIDO
155	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en PHP Session ID	REQUERIDO
156	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en JSP Session ID	REQUERIDO
157	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por SSL session ID	REQUERIDO

CONDICIONES Y ACUERDO DE NIVEL DE SERVICIO

El Proveedor se compromete a cumplir el siguiente "Acuerdo de Nivel de Servicio", bajo los siguientes términos:

- Los plazos para atención a solicitudes de asistencia técnica se determinarán de acuerdo al grado de criticidad y conforme a la severidad de problemas. La definición respecto al nivel de criticidad será determinada exclusivamente por la convocante en la solicitud de soporte.
- En caso de alguna falla en un equipo o bien suministrado, que impida su correcto uso o funcionamiento, se deberá prever un tiempo máximo de respuesta de 2 (dos) horas a partir de la comunicación, por correo electrónico u otro medio, de la convocante al proveedor. En este periodo de tiempo, la empresa debe gestionar los recursos necesarios y empezar a trabajar en la solución del evento.
- En caso de que un equipo presente fallas y no pueda ser reparado se deberá proveer, en carácter temporal- uno igual o de mayores prestaciones hasta la devolución del equipo reparado; se deberán dejar en funcionamiento todos los servicios con todas las configuraciones respectivas. Este soporte es solicitado por el tiempo que dure la Garantía.
- Además, se deberá incluir la revisión, backup, actualización y verificación a pedido de la convocante, acerca del funcionamiento periódico de todo el Hardware/Software utilizados y los cambios de elementos/partes que así lo requieran en el momento y hora definido por la convocante.
- Los servicios solicitados por parte de la convocante o que sean necesarios y que involucren a los bienes y servicios objeto de la presente licitación, deberán ser proveídos por los técnicos propuestos en la oferta y no podrán ser reemplazados sin el consentimiento de la convocante.

TIEMPO DE RESPUESTA A INCIDENTES QUE AFECTAN LA DISPONIBILIDAD DEL SERVICIO

La convocante indicará los servicios/sistemas que serán considerados como críticos y no críticos y que serán atendidos en los siguientes plazos:

- Tiempo de respuesta a servicios/sistemas críticos: 2 (dos) horas desde la comunicación del incidente.
- Tiempo de respuesta a servicios/sistemas no críticos: 4 (cuatro) horas desde la comunicación del incidente.

Para los servicios/sistemas críticos, el Proveedor está obligado a proporcionar y mantener funcionando un esquema de respaldo/contingencia de características iguales o superiores, mientras dure la reparación y puesta a punto del servicio o equipo.

El oferente deberá contar con un Centro de Atención al Cliente propio de la empresa y que sea con funcionalidad operativa 7x24 (24 horas del día, los 365 días del año).

SITUACIÓN ACTUAL

El edificio de la Dirección General de los Registros Públicos, ubicada en las calles Avda. Eusebio Ayala c/ Capitán Román García, cuenta con un edificio de 6 (seis) pisos. En cada uno de ellos, los funcionarios cuentan con sus computadoras personales, impresoras y equipos multifunción, todos éstos conectados a la red interna, totalizando aproximadamente 500 puestos de trabajo, siendo los pisos más densamente poblados la Planta Baja, el Entrepiso y el Primer Piso.

En cada piso, se ubican uno o más gabinetes de comunicaciones (rack), así como varios switches por piso como se describe en la tabla más abajo. Cada uno de los pisos tiene montado y operativo -al menos- dos cables de fibra óptica multimodo de 6 pelos y cada piso cuenta con su correspondiente DIO (Distribuidor Interno Óptico), en su gabinete respectivo.

Piso	Descripción	Cantidad de Switches
1	Planta Baja	5
2	Entrepiso	4
3	Primer Piso	7
4	Segundo Piso	2
5	Tercer Piso	1
6	Cuarto Piso	1
TOTAL		**20**

Descripción de pisos y cantidad de switches por piso

Como se muestra en la tabla superior, todos los pisos cuentan con varios switches de acceso y al menos uno de ellos con interfaces de fibra óptica de corta distancia (SFP), que permiten la conexión de cada piso con el equipo concentrador (switch core), que se encuentra en la Planta Baja y que a su vez se conecta al “Centro de Datos” (datacenter) ubicado en el Entrepiso de la Institución, y en donde funcionan los servicios y sistemas accedidos por los funcionarios y clientes externos.