ANEXO A4

Servidor virtual Filtro para Correo Electrónico (Antispam)

MARCA	
MODELO	
NUMERO DE PARTE DEL FABRICANTE	
CANTIDAD	

Característica	**Fuente (**Folletos, brochures, certificados, enlaces web, catálogos, instructivos, hojas de datos y/o manuales técnicos, o carta del fabricante.**)**	**Pág.**	**Ítem, numeral, capítulo de la pagina**	**Indicar texto o párrafo donde se evidencie cumplimiento de la característica solicita.**
I. Servidor virtual Filtro para Correo Electrónico (Antispam)				
A. Características generales				
1. Debe proporcionar reportes/gráficas de cantidades de correo detectados según categoría de mensajes como Spam, Malware, mensajes maliciosos, recipientes inválidos, mensajes limpios, etc.				
2. Reportes top de usuarios según cantidad de correos recibidos o enviados, detalles del flujo de sus correos y búsqueda por usuario.				
3. Reportes de resultados de análisis de Antivirus, Anti-Malware Avanzado, Filtros de Outbreaks (contagios) incluyendo intentos de Phishing, entre otras amenazas.				
4. Reportes de alto volumen de correo en base a diferentes parámetros como remitente, top subjects, top filtros de mensaje.				
5. Reportes para verificar la capacidad y carga del sistema en diferentes rangos de tiempo, que describen cantidad de conexiones totales entrantes/salientes, promedio de tamaño de correo entrante/saliente, tamaño total de correos, utilización de recursos.				
6. Reportes de los estados de las diferentes cuarentenas, con opciones para tomar acción sobre mensajes determinados.				

7. Capacidad de calendarizar, enviar y archivar reportes.				
8. Rastreo detallado de correos electrónicos: Capacidad de poder hacer búsqueda de un mensaje procesado y poder ver su característica/composición y su detalle cronológico del procesamiento recibido durante el flujo.				
9. Todas las funcionalidades anteriores deben ejecutarse desde la consola de gestión centralizada que permitirá que la solución opere en modo activo-activo				
10. Debe proveer un componente para enviar correos de prueba, simulando Phishing o ataques de ingeniería social. Se deberá detectar si el usuario abrió el correo electrónico y mostrar estadísticas al respecto. Esta funcionalidad puede ser brindada por la propia marca o marca de terceros siempre y cuando cumpla con todo lo solicitado.				
B. Gestión y monitoreo.				
1. Para facilitar la gestión en despliegue de múltiples appliances ya sean físicos y/o virtuales, capacidad para centralizar funciones como reportes, cuarentenas y bitácoras de rastreo de mensajes.				
2. Capacidad de alertar vía e-mail, hacia diferentes destinatarios dependiendo de la categoría y severidad de la alerta.				
3. Capacidad de generar bitácoras (logs) en varias categorías (Anti-Spam, Anti-Malware avanzado, Cuarentenas, etc.) y niveles de criticidad, y diferentes subscriptores dependiendo del tipo de log.				
C. Manejo de Correo de Alto Volumen.				
1. Capacidad de crear filtros de mensajes en base a múltiples parámetros, que permitan la detección de e-mail en alto volumen y aplicar acciones como cuarentena y descartado (drop).				
2. Poder aplicar rate-limiting selectivo tanto en flujos entrantes como salientes.				
3. Poder aplicar throttling de mensajes por remitente, destino o Gateway Virtual, en base a límites configurables.				
4. Poder aplicar excepciones a este tipo de reglas. También se permitirá realizar excepción de control de retransmisión de correo entrante o conexiones por IP address o búsqueda de DNS reversa.				
F. Servicios de Seguridad Generales				
1. Determinar la acción de entrega, cuarentena, etiquetado, descartar o rebotar mensajes de mercadeo.				
2. Debe cómo los mensajes que han caído en uno de los múltiples tipos de cuarentena, pueden recibir acciones predeterminadas, como retención y liberación manual o automática después de cierto intervalo de tiempo				
G. Outbreak Filters y Anti-Phishing				
1. Tener cómo se puede proteger ante ataques mezclados "Blended Threats" por medio de reescribir URLs dentro de mensajes sospechosos. Cuando se da clic, los URL se redireccionan automáticamente a la solución de Web Security del				

mismo fabricante, el contenido se escanea, y se desplegará una pantalla de bloqueo si el sitio contiene malware.				
J. Cifrado/Descifrado de correo electrónico.				
1. Capacidad para enviar correos encriptados al exterior de la organización. El usuario remitente puede especificar qué correo debe de ser encriptado, utilizando alguna palabra clave en el Subject, tal como [CIFRAR].				
2. Capacidad para encriptar el correo automáticamente en base al contenido del correo especificado por alguna regla de DLP, diccionario o regla de contenido.				
3. El correo podrá ser visto por el destinatario después de introducir un usuario y contraseña válidos (que el podrá establecer registrándose en el Servicio de Cifrado, servicio también integrable con gateways SAML 2.0 o en su defecto permitan al destinatario leer los mensajes previo autoregistro en la misma plataforma ofertada.				
4. Capacidad de hacer recall de mensajes encriptados y establecer expiración para revocar la apertura de tales mensajes, pudiéndose cubrir dicha funcionalidad con un componente adicional que forme parte de la solución ofertada				
5. S/MIME y/o PXE y/o componente de cifrado de correos al cuál se pueda acceder por usuario y password generado por el usuario destinatario.				