SERVICIO DE ACTUALIZACIÓN, SUSCRIPCIÓN Y SOPORTE DEL DISPOSITIVO DE SEGURIDAD PERIMETRAL DE LA PLATAFORMA DE MENSAJERIA INSTITUCIONAL DEL MINISTERIO PÚBLICO

I. ANTECEDENTES

La infraestructura del Ministerio Público posee una solución integrada de hardware y software dedicada a proteger la plataforma de mensajería institucional, marca Barracuda, modelo 600, dicho equipo se encuentra en el IDC de Cable & Wireless.

La suscripción y soporte actual finaliza el 13 de octubre del presente año.

II. OBJETIVO GENERAL

Adquirir la suscripción y servicio de soporte de la solución dedicada a proteger la plataforma de mensajería institucional de ataques de denegación de servicios, de correo no deseado (spam), Phishing, virus y de suplantación de identidad (spoofing).

III. OBJETIVOS ESPECÍFICOS

- Contratar el servicio de suscripción de actualizaciones de software a tres años.
- Suscripción de reemplazo de equipo de fábrica ante daños físicos o lógicos a tres años.
- Cobertura de soporte de parte de ingenieros certificados en la solución ofertada por tres años.

IV. JUSTIFICACION DE LA SOLICITUD

El correo malicioso resulta con frecuencia peligroso, ya que los correos indeseados sirven como un medio para distribuir malware y otros tipos de amenazas, por ello se debe fortalecer la infraestructura para proteger la plataforma de mensajería institucional de ataques que puedan causar daños masivos e irreversibles.

V. COMPONENTES DE CONTRATACIÓN

- Suministrar soporte con respecto al funcionamiento de la solución por tres (3) años.
- Suministrar suscripción de tres (3) años tipo "Energize Updates – Basic Support" al Barracuda Spam Firewall 600.
- Suministrar suscripción de tres (3) años tipo "Instant Replacement - Enhanced Support" del Barracuda Spam Firewall 600.

VI. ESPECIFICACIONES TÉCNICAS

Las soluciones ofertadas deberán cumplir con todos y cada uno de los requerimientos técnicos detallados a continuación:

- La solución debe ofrecer protección del servicio de correo en múltiples capas, utilizando técnicas de filtrado de conexiones y escaneo profundo en los mensajes.
- La solución debe ser capaz de brindar protección que permita rechazar el correo no deseado (spam), mediante la previa verificación y comprobación de las direcciones ip de mensajería entrante, en bases de datos especializadas con registros de sitios considerados como altamente generadores de "spam".
- La solución deberá poseer mínimo 2 capas de protección antivirus.
- La solución debe de hacer cache de firmas de antivirus localmente y automáticamente actualizable.
- La solución debe ofrecer protección en tiempo real que bloqueará nuevos spam y los virus en tiempo real, sin tener que esperar que nuevas definiciones estén descargadas en el appliance.
- La solución deberá ser capaz de proteger correo electrónico entrante (desde Internet) y correo saliente (hacia Internet), protegiendo a la organización de amenazas y evitando de esta forma que se pierda información sensible.
- La solución deberá ser capaz de conectarse en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones.
- La solución debe contar con protección contra ataques de negación de servicio.

- La solución debe ser capaz de realizar verificaciones de DNS en reversa para proveer protección tipo Anti-Spoofing
- La solución debe ser capaz de establecer límites en la tasa de correos enviados y recibidos.
- La solución debe contar con la capacidad de soportar múltiples dominios de correo electrónico.
- La solución debe permitir establecer políticas de correo electrónico por dominio, para correo entrante o correo saliente.
- La solución debe ser capaz de establecer perfiles (políticas) granulares de detección de SPAM.
- La solución debe ser capaz de realizar enrutamiento de correo basado en LDAP.
- La solución debe contar con la capacidad de poder hacer cuarentena de correo entrante y saliente.
- La solución debe contar con soporte a colas de correo para mensajes fallidos, retardados y no entregables.
- La solución debe poder hacer autenticación para SMTP a través de LDAP, RADIUS, POP3 o IMAP.
- La solución debe ser capaz de realizar filtraje de archivos anexos (attachments) y contenido de mensaje de correo.
- La solución debe estar en capacidad de bloquear usando listas RBL de SPAM.
- La solución debe permitir el filtraje por palabra prohibida.
- Administración de SPAM con capacidades de Aceptar, Reenviar (Velay) Rechazar (Reject) o descartar (discard).
- Rastreo por análisis de imágenes para detectar SPAM.
- Listas negras y blancas (usuarios/dominios/ direcciones IP).
- La vigencia de la licencia de actualización deberá incluir la capacidad de poder hacer actualizaciones de firmas antispam, antivirus y cualquier otra actualización necesaria para la correcta operación del equipo.
- Bloqueo de spam en otros idiomas.
- Deberá generar información del uso del filtro de SMTP, la cual debe poder ser leída y explotada por otro dispositivo mediante formato syslogs, txt y/o csv o xls sin generar una afectación a la continuidad del servicio.
- Interface de configuración vía Web (HTTP, HTTPS).
- Los administradores podrán ser por dominio y deberá poder asignarse de qué equipos (por dirección IP y máscara) puede el administrador conectarse.
- Soporte a por lo menos dos niveles de administración: lectura / escritura (Read/Write) y sólo lectura (Read-Only).
- Soporte a SNMP versión 1 / versión 2 usando MIBS estándares y MIBS privados con Traps basadas en umbrales.
- Soporte a registro (logging) de actividad antispam.
- Soporte a syslog externo.
- Deberá poseer al mínimo 10 reportes diarios.
- Deberá generar reportes bajo demanda o calendarizados en intervalos específicos.

- Los reportes pueden ser generados y enviados como PDF.
- Soporte a capacidades de configuración de equipos en Activo-Activo o Activo-Pasivo utilizando MX records o Network Load Balancer.
- Soporte a sincronización de políticas y registros de log de mensajes de correo.
- Capacidad de protección de tráfico de correo basándose en los tipos MIME en los archivos anexos.
- La solución debe permitir a los usuarios establecer la lista blanca de remitentes y marcar mensajes como spam y no spam directamente desde clientes Microsoft Outlook y Lotus Notes.
- La solución debe ofrecer a los usuarios la capacidad de la lista blanca / lista negra de remitentes, así como gestionar su propio correo no deseado.
- La solución debe ser capaz de realizar búsquedas federadas a través de los registros entre aparatos distribuidos.
- La solución debe tener la capacidad para los administradores de bloquear mensajes de correo electrónico a través de la cabecera / sujeto / body utilizando expresiones regulares expresiones y coincidencias de palabras exactas.
- La solución debe ser capaz de bloquear los archivos adjuntos por tipo de archivo y extensión de archivo.
- La solución debe tener la capacidad de obligar conexión SMTP a través de TLS al enviar o recibir correo electrónico de un dominio específico.
- La solución debe tener la capacidad de utilizar una base de datos de direcciones IP y dominios para ayudar a bloquear el spam.
- La solución debe ser capaz de bloquear los mensajes de devolución / NDR.
- La solución debe tener la capacidad para hacer cumplir la política de correo electrónico basado en el tipo de caracteres en las partes del mensaje.
- La solución debe ser capaz de realizar una búsqueda DNS inversa en la dirección IP del remitente, determinar el Top Level Domain (TLD) y correos electrónicos de bloques procedentes de direcciones IP asignadas a los proveedores en países conocidos comúnmente de enviar spam.
- La solución debe permitir a los administradores crear reglas personalizadas basadas en los resultados de búsqueda de DNS inversa de la dirección IP del remitente.
- La solución debe ser capaz de hacer cumplir la política de correo electrónico mediante la comprobación del servidor de nombres de un dominio de referencia en URL incrustado y validación frente a una lista de servidores de nombres conocidos de ser utilizado exclusivamente por spammers.
- La solución debe ser capaz de hacer cumplir la política de correo electrónico mediante la inspección del contenido de sitios web gratuitos vinculados a los URL en los mensajes de spam.
- La solución debe ser capaz de evitar que los spammers envíen grandes cantidades de correo electrónico al dispositivo a través de un corto período de tiempo desde cualquier dirección IP.

- La solución debe ser capaz de utilizar SNMP para la supervisión y alertas y utilizar una API para hacer cambios de configuración sin tener que entrar en el aparato.
- La solución debe ser capaz de proporcionar la seguridad de correo electrónico híbrido; nube de pre-filtrado de tráfico de correo electrónico entrante para detener el spam y el malware con la entrega de correo electrónico pre-filtrado en un appliance local. El uso de la nube de pre-filtrado no debe acarrear ningún costo adicional.
- La solución debe ser capaz de proporcionar la continuidad de correo electrónico a través de la cola en la nube y la entrega a un servidor de correo electrónico alternativo.
- La solución debe incluir el cifrado de correo electrónico saliente, especificado por una política configurada en el appliance local y entregado a través de una nube segura del fabricante. Esta función no debe acarrear ningún costo adicional.
- La solución debe ser capaz de proporcionar una protección antivirus de correo electrónico interno dentro de Microsoft Exchange con un agente que se instala en los servidores de Exchange y que se sincroniza con el appliance local.
- La solución debe ser capaz de recibir correos electrónicos de redes IPv6, aplicar políticas de contenido y entregar a cualquier red IPv4 o IPv6.

SOPORTE TÉCNICO

- El proveedor debe dar soporte con respecto al funcionamiento de la solución por treinta y seis (36) meses, 24/7 para emergencias y 8x5 en sitio, así como proveer información de contacto con escalamiento.
- El proveedor debe ofrecer apoyo en las actualizaciones de las aplicaciones y software con hardware.
- Realizar revisión de funcionamiento trimestralmente por parte del proveedor en el sitio de la instalación.
- El proveedor debe ofrecer soporte telefónico y por correo electrónico.
- El proveedor debe ofrecer soporte en sitio en dos (2) horas para casos críticos.
- Suscripción de Soporte Colaborativo del proveedor de los equipos de seguridad perimetral de Ministerio Público.

IMPLEMENTACIÓN

- El personal de la Dirección de Informática del Ministerio Público estará encargado de supervisar y administrar cada etapa de la actualización.

- La labor de actualización no debe afectar el normal funcionamiento de los equipos que se encuentran en producción, de requerirse por fuerza mayor la interrupción de la conectividad del Ministerio Público al internet deberá ser planificada la ventana de mantenimiento con el personal de la Dirección de Informática y cuantificar su duración.

GARANTÍA

- Los trabajos a realizar sobre la plataforma deberán poseer una garantía mínima de tres (3) años.
- En caso de que se deba revisar el equipo en los talleres del proveedor, se debe reemplazar los equipos en un periodo no mayor de dos (2) horas, y este debe poseer las mismas configuraciones del primero.
- Dicha garantía incluirá la actualización de las versiones del programa u otro tipo de actualizaciones requerida para que la solución integral de los servicios funcione adecuadamente, debe ser instalada, configurada, actualizada y monitoreada por el proveedor.
- El proveedor debe detallar la garantía, mantenimiento del hardware en fallas imputables a la empresa. Este plan de garantía debe incluir lo siguiente:
  - Reparación de errores.
  - Instalación de nuevas actualizaciones por incumplimiento de los términos de referencia y/o errores.
  - Tiempo de respuesta oportuno. Seguimiento y disposición por parte del proveedor del cumplimiento de corrección de errores y/o comportamiento esperado del sistema.
  - El sistema no puede estar inactivo más de cuatro (4) horas siendo una garantía de compromiso que le proveedor debe asegurar.

VII. REQUISITOS DEL PROVEEDOR

- El proponente deberá tener sus oficinas en la República de Panamá debidamente establecida con una estructura bien definida y organizada.
- El proponente deberá tener experiencia de más de diez (10) años en la representación de la marca a nivel nacional.
- El proponente debe tener como personal permanente en el territorio nacional un mínimo de cuatro (4) ingenieros certificados por el proveedor en nivel experto (presentar certificados).
- El proponente debe tener experiencia en soporte a instalaciones de más de mil (1,000) usuarios.

- El proponente deberá poseer la certificación como socio de negocios avanzados (Gold, Platinum) del fabricante con la certificación de proveedor de soporte autorizado.
- El proponente deberá tener la capacidad de reemplazar el equipo en caso de falla, con otro de las mismas características o superior en calidad de préstamo, en un periodo no mayor a veinticuatro (24) horas, hasta que llegue el equipo nuevo.
- El proponente debe tener una estructura de atención de incidentes que contemple el soporte remoto y en sitio.

VIII. TIEMPO DE ENTREGA

La entrega del producto está sujeta a la generación de la orden de compra por el Ministerio Público y a la notificación del proveedor. El servicio contratado debe iniciar el 14 de octubre del presente año.

IX. PRECIO DE REFERENCIA

El costo estimado es por la suma de treinta y un mil quinientos con 00/100 (B/. 31,500.00).