ANEXO III

PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN, MEDIANTE PROCEDIMIENTO SIMPLIFICADO, DEL SUMINISTRO DE LICENCIAS DE PROTECCIÓN DE SPAM Y MALEWARE Y LICENCIAS DE PROTECCIÓN AVANZADA CONTRA AMENAZAS (ATP) PARA EL SISTEMA DE CORREO ELECTRÓNICO DEL PARLAMENTO DE NAVARRA.

1.- OBJETO DEL CONTRATO

Desde el año 2015 el sistema de correo electrónico del Parlamento de Navarra cuenta con un sistema de seguridad y protección para luchar contra el spam, phising y las listas negras. El licenciamiento actual es 180 licencias de Cloud Email Firewall y 180 licencias Advanced Threat Protection (ATP) SPAMINA.

La empresa Spamina asociada a HornetSecurity ha evolucionado sus productos, el Cloud Email Firewall equivale al producto Spam and Malware Protection y el producto Advanced Threat Protection (ATP) SPAMINA equivale a Advanced Threat Protection.

El spam, que representa más del 50 % de todo el tráfico de correo electrónico, es el método más intrusivo con que los ciberdelincuentes intentan introducir malware y virus en los sistemas corporativos. La instalación de un software con funciones y mecanismos de filtro de protección contra spam y malware mantienen el buzón del correo electrónico libre de molestos y dañinos mensajes de spam.

El riesgo de un ataque cibernético de secuestro de datos, fraude del CEO y troyanos aumenta cada vez más. Por ello, se hace necesario contar con protecciones de tipo Advanced Threat Protection (ATP).

Parlamento de Navarra requiere ahora la renovación de las licencias indicadas y además del soporte del fabricante, necesita el servicio profesional de soporte técnico por parte del Partner, con acuerdo de SLA, que dé apoyo y ejecute las actuaciones necesarias tanto para resolver incidencias como para realizar tareas de mantenimiento preventivo y evolutivo.

2.- LICENCIAS A CONTRATAR

A continuación, se indica la relación de licencias a incluir en el contrato:

DESCRIPCIÓN	**UDS.**	**DURACIÓN**
Spam and Malware Protection (HornetSecurity)	180	1 año
Advanced Threat Protection (HornetSecurity)	180	1 año

3.- CARACTERÍSTICAS DEL SERVICIO SOPORTE POR PARTE DEL PARTNER

Es imprescindible que el Partner esté registrado como “Partner de HornetSecurity”, con el fin de garantizar el buen acceso a la información y a formación especializada por parte de HornetSecurity. En el caso que el Partner subcontrate a un tercero para los servicios de SOC, éste último debe también ser Partner registrado para poder tener acceso a la formación oficial de HornetSecurity.

El soporte de HornetSecurity funciona en un sistema 24/7 y está disponible todos los días del año.

La propuesta de servicio por parte del Partner ha de comprender las siguientes tareas:

- Gestión y atención de incidencias, el soporte de primer nivel será ofrecido directamente por el Partner y, de ahí en adelante, el resto de niveles (L2 y L3) los ofrecerá HornetSecurity.
- Atención a consultas del servicio.
- Apertura y seguimiento de casos con el fabricante.
- Recomendación de metodologías para implantar.
- Asesoramiento y suministro de información ante consultas sobre nuevas actualizaciones.
- Actualización correctiva de versiones ante bugs reconocidos por el fabricante que acaben repercutiendo en una incidencia o indisponibilidad de servicio.
- Asesoría técnica, en caso de requerirse.
- SLA de 4 horas de respuesta de lunes a viernes en horario de 08.00h a 18.00h.