



AYUNTAMIENTO DE CUENCA

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR PARA LA CONTRATACIÓN DE LA PRESTACIÓN DEL SERVICIO DE FILTRADO DE CORREO ELECTRÓNICO.



1.- OBJETO Y ALCANCE DEL CONTRATO

1.1. Objeto

El Ayuntamiento de Cuenca en su proceso de mejora continua de la seguridad pretende, mediante esta contratación, securizar más una de las vías por las cuales se realizan la mayoría de los ataques que es el correo electrónico.

Entre las principales amenazas se encuentran las siguientes:

Malware: software malicioso tal como virus, troyanos, gusanos o cualquier código o contenido que pueda tener un impacto adverso en organizaciones o individuos.

Ransomware: un tipo de malware que bloquea los sistemas o los datos de los ordenadores de sus víctimas, permitiéndoles el acceso una vez que se satisface un pago (extorsión).

Phishing: correos electrónicos que simulan proceder de un organismo público o de una persona, persiguiendo extraer información sensible de los ciudadanos, del propio Ayuntamiento o sus responsables o empleados.

Ingeniería social: recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, etc.

Explotación de vulnerabilidades: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de las vulnerabilidades organizativas o técnicas del sistema atacado.

Acceso no autorizado a la información: sustracción de credenciales de acceso.

El objeto del presente pliego es la contratación de los servicios para el **filtrado avanzado del correo electrónico** del dominio **cuenca.es**, con el objeto de reducir al máximo las amenazas, reduciendo la posibilidad de que un correo electrónico dañino pueda llegar al usuario final.

1.2. Alcance

El Ayuntamiento de Cuenca dispone de un servicio de correo electrónico On-Premise, gestionado por el Área de Sistemas Informáticos, en el cual se realizan filtrados de correo electrónico con el objeto de reducir la amenazas indicadas anteriormente. Dicho filtrado se considera insuficiente antes los ataques cada vez más sofisticados que se están realizando a diferentes empresas privadas y entidades públicas.

El alcance del presente contrato son los servicios para el **filtrado avanzado del correo electrónico** del dominio **cuenca.es**, para un mínimo de **600** cuentas de correo, con el objeto de reducir al máximo las amenazas, reduciendo la posibilidad de que un correo electrónico dañino pueda llegar al usuario final.

2.- REQUISITOS

2.1. Requisitos Generales

- La solución deberá estar basada en arquitectura altamente disponible que permita garantizar el nivel de servicio acordado.
- La solución deberá ser ofrecida directamente desde la infraestructura del proveedor, es decir, que no se deberá instalar equipos en la red interna del Ayuntamiento.
- La arquitectura utilizada garantizará la capacidad de escalado de la solución, permitiendo iniciar el despliegue en un entorno ajustado a las necesidades iniciales del Ayuntamiento y que evolucionará conforme se requiera.

Además de la seguridad, es de gran importancia para el Ayuntamiento de Cuenca la continuidad y disponibilidad del servicio de correo electrónico, por ello aun que **no es objeto de este contrato**, en el caso que el servicio de correo electrónico del ayuntamiento no funcione por algún motivo y no pueda ser levantado en un corto período de tiempo la solución deberá permitir la incorporación de forma ágil y rápida de los siguientes servicios para el caso de que el ayuntamiento se vea en la necesidad de contratarlos en algún momento:

- La solución deberá poder integrar los servicios de filtrado de correo con servicios de archivado y encriptación de correo.
- La solución deberá de ser capaz de proporcionar Disaster Recovery para el correo electrónico. En caso de caída del servidor de correo del ayuntamiento de Cuenca, cada usuario podrá tener a su disposición una bandeja de entrada y salida para poder utilizar el correo electrónico.



2.2. Requisitos Filtrado

En general se busca una solución perimetral para el filtrado de spam, virus y contenido no deseado en tráfico SMTP (correo electrónico). Deberá proteger, escanear y filtrar el correo entrante y saliente. Deberá soportar la tecnología de cifrado TLS (Transport Layer Security), al menos en versión TLS 1.2.

2.2.1. Filtros de Conexión.

En este apartado se valorará el funcionamiento para la característica que permite o bloquea el correo electrónico en función del origen del mensaje. Filtrado de conexiones, en base a la dirección IP del servidor que realiza la conexión para determinar la acción.

En resumen el filtrado de conexiones es el primer paso contra correo no deseado en evaluar un mensaje entrante. La dirección IP de origen de la conexión SMTP se comprueba según las direcciones IP permitidas y bloqueadas. Si la dirección IP de origen se ha permitido de forma específica, el mensaje se envía a los destinatarios de la organización sin que otros agentes contra correo no deseado lleven a cabo ningún procesamiento adicional. Si la dirección IP de origen se ha bloqueado de forma específica, la conexión SMTP se cancelará. Si la dirección IP de origen no se ha permitido o bloqueado de forma específica, el mensaje fluye a través de los demás agentes contra correo no deseado.

El filtrado de conexiones ha de comparar las dirección IP del servidor de correo de origen con los valores en la lista de direcciones IP permitidas, la lista de direcciones IP bloqueadas, los proveedores de la lista de IP permitidas y los proveedores de la lista de IP bloqueadas, etc.

2.2.2. Filtros antimalware.

En este apartado se valorará y diseño y funcionamiento del agente antimalware para detectar todo el malware conocido. Los mensajes que se transportan a través del servicio de correo se analizaran en busca de malware (virus y spyware).

En resumen si se detecta malware, se elimina el mensaje, se poden en cuarentena etc, las notificaciones han de poder enviarse a remitentes o administradores cuando se elimina un mensaje infectado y no se entrega, también se ha de poder elegir sustituir los datos adjuntos infectados por mensajes predeterminados o personalizados que informan a los remitentes de la detección del malware.

2.2.3. Filtros de contenido antispam.

En este apartado se valorará el filtrado Anti-Spam que se encargue de analizar el correo que, intentando identificar aquellos mensajes que son Spam (Se llama Spam o 'correo basura' a los mensajes de email que se reciben, generalmente con publicidad, y que son enviados de forma masiva por personas o empresas a





los que no hemos facilitado nuestra dirección de correo.) para eliminarlos o separarlos de los demás, de tal forma que nuestro buzón de correo no se vea afectado por estos mensajes no deseados.

2.2.4. Filtros anti-phishing.

El servicio ha de intentar bloquear las actividades de phishing. En este apartado se valorará el filtrado antiphishing que ofrece el servicio a contratar.

Es importante que el filtro antiphishing realice un buen filtrado pero que además no sea demasiado entusiasta para que no bloquee el correo electrónico legítimo.

2.2.5. Filtros de amenazas avanzadas (ATP).

Los requisitos de filtros vistos hasta ahora son los considerados como básicos que ha de disponer la herramienta, dichos filtros ya se están realizando en mayor o menor media por el servidor de correo del ayuntamiento, el servicio que se solicita en este apartado consiste en una seguridad más avanzada, más allá del típico filtro basado en bases de datos con firmas de amenazas conocidas.

Técnicas de detección heurísticas, protección ante virus desconocidos (hora cero), amenazas por comportamiento, análisis de URL's en el momento en el que el usuario abre el enlace no solamente en el momento en el que recibe el enlace, etc.

2.2.6. Filtros de prevención de suplantación de identidad.

La solución ofertada debe proporcionar una protección efectiva frente a intentos de suplantación de identidad dirigidos a personal de alto valor dentro de la organización (whaling / spear phishing), identificando por ejemplo:

El uso fraudulento de nombres de personas del Ayuntamiento.
El uso fraudulento de direcciones electrónicas del Ayuntamiento.
Análisis de patrones de contenido
Verificación de integridad y autenticación.

2.2.7. Alertas.

En este apartado se valora el sistema de alertas disponible por la herramienta, avisos a los administradores en tiempo real, avisos al usuario, categorización de las alertas etc.

2.2.8. Administración de la Solución.

En esta apartado se valora la solución para gestionar y administrar la herramienta, el panel de control, los perfiles de usuario para gestionar los correos puestos en cuarentena, listas negras, listas blancas, configuración de los reportes, informes para realizar las diferentes tareas de administración, la gestión de los correos filtrados, análisis del tráfico en tiempo real, sistema de trazas y logs, backup desde consola del servidor de correo del ayuntamiento, etc.

3. CONDICIONES DE EJECUCIÓN

La ejecución material de los servicios se realizará con estricta sujeción a las cláusulas estipuladas en el contrato, en el pliego de prescripciones técnicas que define los trabajos y en la propuesta que el adjudicatario haya hecho en su oferta técnica.

El adjudicatario deberá prestar los diferentes servicios contratados aplicando siempre la diligencia exigible a las buenas prácticas del sector, y conforme a las instrucciones que en interpretación del contrato diese el responsable del contrato o el órgano de contratación.

Las actuaciones de seguimiento y control de la ejecución material del contrato se realizarán sin perjuicio de los controles administrativos sobre la ejecución formal y documental del contrato que realicen los Servicios municipales de Contratación e Intervención, que a su vez podrán solicitar al Responsable municipal del contrato comprobaciones puntuales del cumplimiento por parte del adjudicatario de determinadas obligaciones y cuantos informes estimen oportunos para comprobar el grado de cumplimiento del contrato por parte del adjudicatario.

La empresa adjudicataria deberá proponer un equipo de trabajo coherente con las tareas propuestas y nombrará un supervisor o responsable de proyecto que actuará como interlocutor con los responsables de la unidad de coordinación y seguimiento del Ayuntamiento de Cuenca.

El adjudicatario deberá aportar personal técnico experimentado en los entornos tecnológicos y funcionales incluidos dentro del alcance del contrato, con categoría profesional y nivel de especialización adecuados a las necesidades planteadas.

El adjudicatario se compromete a que la rotación en su personal no afecte en absoluto a la calidad del servicio prestado.

4.- ACUERDO DE NIVEL DE SERVICIO Y SOPORTE

La tasa de detección de spam mensual ha de ascender como mínimo al 99% de media en relación a todos los correos recibidos por el dominio cuenca.es en el periodo analizado.

La tasa de detección de virus media anual ha de ascender como mínimo al 99% respecto a los correos recibidos por dominios del cliente en el periodo analizado.

La disponibilidad en el tráfico de correo vía SMTP ha de ascender como mínimo al 99% de media anual. Esto requiere que todos los correos entrantes se envíen directamente por SMTP a los sistemas mediante modificación de los registros MX del dominio cuenca.es.

El sistema ha de ser lo suficientemente eficiente para tener un número de falsos positivos mínimo, pues como se ha indicado anteriormente la seguridad en el filtrado del correo electrónico es muy importante pero este filtrado no puede llevar a que no se reciban o se reciban con mucho retraso o se reciban en carpetas de spam o de cuarentena correo limpios.

Por ello La tasa de falsos positivos media mensual ha de situarse como mínimo por debajo del 0,00020% respecto a los correos limpios recibidos por el dominio cuenca.es.

En el cálculo de la disponibilidad no se incluyen las labores de mantenimiento planificado, siempre y cuando sean comunicadas al ayuntamiento de Cuenca con una antelación mínima de 3 días, estas labores de mantenimiento se efectúan, en la medida de lo posible, en horario nocturno, durante los fines de semana.

El soporte tiene que ofrecido en español y no por procesos automatizados como por chatbos.

Cuenca, en fecha de firma electrónica