AYUNTAMIENTO DE CUENCA

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR PARA: CONTRATACIÓN DEL SERVICIO DE CIBERSEGURIDAD.
SOC (Centro de Operaciones de Seguridad)

OBJETO Y ALCANCE

1.- Objeto del contrato

El Ayuntamiento de Cuenca tiene desplegada desde 2023 una plataforma SIEM donde se recogen todos los eventos de seguridad que se registran en la infraestructura municipal. Sistema de seguridad de la información y gestión de eventos de seguridad SIEM. (SECURITY INFORMATION AND EVENT MANAGEMENT). Todos estos eventos deben ser monitorizados 24x7x365 para poder hacer frente a las continuas amenazas que todas las administraciones reciben y que van en aumento.

El objeto de esta contratación es un Servicio gestionado de ciberseguridad adecuado a las necesidades municipales y alineado con el objetivo principal de proteger los activos críticos y sistemas de información necesarios para el funcionamiento del ayuntamiento, minimizando los incidentes de seguridad y promoviendo la mejora continua, para ello se necesita disponer de un Servicio de Operaciones de Seguridad ante amenazas y una respuesta rápida ante incidentes de seguridad, en modalidad de 24x7x365.

Este servicio no solo se centra en la monitorización, vigilancia y protección, sino en la mejora continua y aplicación de las mejores prácticas, aumentando el nivel de madurez en ciberseguridad día a día.

2.- Alcance del contrato

2.1.- Servicios Incluidos

2.1.1. Servicio de soporte y mantenimiento de la plataforma

El adjudicatario llevará a cabo la monitorización de disponibilidad de la plataforma, será el responsable del mantenimiento correctivo, adaptativo y evolutivo de todos los componentes instalados, excluyendo el hardware que sea propiedad del Ayuntamiento de Cuenca sobre el que se encuentran instaladas la(s) máquina(s) virtual(es) de la solución. También será el encargado de llevar a cabo dichas actualizaciones siempre previa autorización del Ayuntamiento.

De especial importancia en este ámbito es el mantenimiento y ajuste de sensores, incluyendo la actualización de reglas de IDS, de filtrado y de correlación, y su optimización para mantener los volúmenes de eventos en niveles aceptables, la minimización de falsos positivos y la activación o desactivación adecuadas de la monitorización de los diferentes sensores.

Todas las actividades necesarias para mantener actualizadas las reglas de monitorización y de correlación, incluyendo la eliminación o modificación de reglas existentes o la creación de nuevas reglas en función de la experiencia adquirida durante la prestación del servicio en el entorno tecnológico del Ayuntamiento de Cuenca.

Igualmente, este servicio será el responsable de actualizar las reglas y adaptar el sistema de monitorización cuando se incorporen o se den de baja elementos de la infraestructura que deban ser monitorizados.

El objetivo de este servicio es el mantenimiento y actualización de las tecnologías desplegadas en el Ayuntamiento, para el funcionamiento de la plataforma SIEM, las sondas de recolección así como de las configuraciones e integraciones realizadas para dar el servicio, como las reglas de correlación, así como el mantenimiento y ajuste de sensores, incluyendo la actualización de reglas de IDS, de filtrado y de correlación, y su optimización para mantener los volúmenes de eventos en niveles aceptables, la minimización de falsos positivos y la activación o desactivación adecuadas de la monitorización de los diferentes sensores.

2.1.2. Servicio de SOC

Servicio 24*7 de Centro de Operaciones de Seguridad (en adelante SOC), que se encargará de la monitorización continua del sistema y gestión de ciberincidentes, además, deberá llevar a cabo el soporte y mantenimiento de la plataforma SIEM existente en el ayuntamiento.

Este servicio incluirá:

2.1.2.1. Service Desk de Seguridad (Oficina de Peticiones de Servicio)

Servicio remoto para el soporte a usuarios finales de los sistemas de información del ayuntamiento que se encargará de la resolución de incidencias, análisis de phishing y muestras, peticiones, consultas, problemas y reclamaciones del usuario relativas a seguridad de la información. Dicho servicio será coordinado a través del Área de Sistemas Informáticos y Comunicaciones.

2.1.2.2. Servicio de boletín de alerta temprana (BAT)

Servicio cuyo objetivo es entregar periódica y puntualmente, en aquellos casos necesarios, un boletín de alerta temprana en el que, en formato de correo electrónico, se nos comunicará cuales son las amenazas y riesgos más incipientes del mercado. Con estos comunicados se podrán tomar las medidas necesarias para prevenir un ciberataque y, en el caso de que este se hubiese producido, ayudar a contener su expansión y minimizar el impacto en el funcionamiento del ayuntamiento.

2.1.2.3. Servicio de gestión contínua de vulnerabilidades

El objetivo es detectar puntos débiles/ciegos en la arquitectura TI a través de la simulación de ataques de vulnerabilidades conocidas. Además de la información sobre configuraciones inseguras en la infraestructura, permite detectar todos aquellos activos que no cuentan con los últimos parches de seguridad publicados por los diferentes fabricantes de hardware y software, priorizar riesgos y aplicar e introducir mejoras de ciberseguridad Detección y Respuesta

2.1.2.4. Servicio de monitorización ante incidentes de seguridad 24x7

Servicio para gestionar los ciberataques, medidas de mitigación y recuperación. El objetivo de este servicio es la recepción, catalogación y análisis de eventos de seguridad (SIEM), identificando aquellos que puedan tener impacto en el ayuntamiento y escalando debidamente las medidas oportunas para mitigar y contener el incidente de seguridad de forma efectiva.

La tecnología SIEM propuesta para el presente servicio debe cumplir los siguientes requisitos:

- Estar posicionada de las primeras dentro de la categoría LEADERS en el cuadrante mágico de Gartner, de productos SIEM (Magic Quadrant for Security Information Event Management).

- La herramienta SIEM debe estar catalogada como ENS ALTA dentro de la familia de Sistemas de Gestión de Eventos de Seguridad en la Guía de Seguridad de las TIC CCN-STIC 105 (catálogo del CCN)

- En la actualidad, el Ayuntamiento de Cuenca dispone de licencias de QRADAR SIEM para la prestación del servicio por parte del actual prestatario. El licitador deberá incluir todo coste asociado al mantenimiento de dichas licencias o a las licencias de la solución propuesta a lo largo de todo el contrato. El licitador deberá hacerse cargo de la migración en caso de cambio de tecnología, migrando todos los casos de uso generados sobre la plataforma actual.

- La plataforma propuesta debe incluir capacidades integradas de orquestación y automatización de operaciones de ciberseguridad (SOAR), así como soporte para automatizaciones basadas en aprendizaje automático (Machine Learning).

- La herramienta SIEM deberá disponer de capacidades de análisis de comportamiento de usuarios y entidades (UBA)

2.1.2.5. Servicio de modelado de amenazas contínuo

Las amenazas a la seguridad cibernética son abundantes y están en constante cambio. Es por eso que el servicio de modelado de amenazas, el diagrama de diversas amenazas e impactos es una práctica crítica y necesaria para prepararse para cualquier amenaza que se presente. El servicio de modelado de amenazas es pieza fundamental para construir un esquema completo de defensa contra amenazas en continua evolución. Al panificar e implementar correctamente los casos de uso resultantes del modelado de amenazas sobre las herramientas del servicio (SIEM, SOAR, etc.), se pretende garantizar que cada rincón y grieta de las infraestructuras y aplicaciones del ayuntamiento permanezca protegido ahora y a medida que surjan nuevas amenazas. El adjudicatario deberá de aplicar los casos de uso creados específicamente para el Ayuntamiento de Cuenca por el actual proveedor.

2.1.2.6. Servicio de respuesta y análisis forense ante incidentes de seguridad

Servicio cuyo objetivo es la ejecución de acciones ordenadas para contener, responder y recuperar de forma eficaz ante un incidente de seguridad. Dichas acciones se llevarán a cabo por un equipo especialista de respuesta ante incidentes y podrán ejecutarse de forma remota o presencial en las sedes de Ayuntamiento de Cuenca, dependiendo del impacto y el acceso a los sistemas de la información.

2.2.- Modalidad del servicio

2.2.1. Servicio de soporte y mantenimiento de la plataforma

Servicio de 8X5

El servicio se dará en modalidad de 8x5, esto es, en horario laboral entre semana. Con independencia de los medios que se establezcan para la atención 24x7, el horario mínimo en el que poder contactar con el personal del contrato será:

■ De lunes a Viernes en horario de 9:00 a 14:00.

Se tomará como referencia el calendario laboral de Cuenca.

2.2.2. Servicio de S.O.C.

SERVICIO DE SOC 24*7

Durante esta fase del servicio, el horario del mismo será de 24 horas los 7 días de la semana y se prestará desde las instalaciones del adjudicatario.

Servicio de detección mediante monitorización activa de la plataforma:

- Recolección, monitorización y correlación de eventos de seguridad procedentes de las fuentes de información integradas, sondas NIDS y agentes HIDS.
- Análisis de eventos y notificación de alertas de seguridad.

Servicio de respuesta ante ciberincidentes:

- Activación de protocolos de actuación.
- Coordinación de la respuesta y definición de las pautas a seguir.

Servicio de prevención

- Alerta temprana: Este servicio consiste en la notificación temprana de la publicación de nuevas vulnerabilidades y actualizaciones de seguridad sobre las tecnologías monitorizadas a través de la plataforma. La gestión de las actualizaciones será responsabilidad del Área de Sistemas Informáticos y Comunicaciones del Ayuntamiento de Cuenca. Las notificaciones se harán directamente a dicha Área según el cauce que el Ayuntamiento de Cuenca y el adjudicatario acuerden.

El servicio deberá utilizar una herramienta de ticketing integrada con el SIEM/SOAR como herramienta de registro y tratamiento de las alertas que sean detectadas por el servicio de monitorización.

El proceso de gestión de incidentes de seguridad o ciberincidentes, establece una clasificación común para todos los incidentes de seguridad. Esta clasificación se basa en los conceptos de IMPACTO y de PELIGROSIDAD, los cuales determinan la PRIORIDAD conforme a la matriz establecida indicada más adelante.

A continuación, se describen los conceptos utilizados y se detalla el significado de los diferentes niveles de IMPACTO y PELIGROSIDAD y el correspondiente factor asociado de PRIORIDAD, bajo los cuales se establecen los niveles de servicio objetivo establecidos para su resolución.

Impacto

Se evalúa el Nivel de Impacto Potencial de los ciberincidentes según lo marcado a nivel nacional (Real Decreto 43/2021, de 26 de enero). Alternativamente, también se considerará impacto crítico aquellos incidentes de seguridad que afecten a la disponibilidad de los servicios IT fundamentales (servicios de directorio activo, ERP, Intranet, correo y acceso a unidades de red).

Nivel	Impacto
1	Bajo
2	Medio
3	Alto
4	Muy Alto
5	Crítico

Peligrosidad

La peligrosidad de los incidentes se determinará según lo detallado en la guía de notificación y gestión de ciberincidentes del CNPIC (Centro Nacional de Protección de Infraestructuras Críticas).

Nivel	Peligrosidad
1	Bajo
2	Medio
3	Alto
4	Muy Alto
5	Crítico

Prioridad

De acuerdo con los códigos descritos de impacto y peligrosidad, se fija la prioridad según el siguiente cuadro.

	Impacto				
Peligrosidad	Bajo	Medio	Alto	Muy alto	Crítico
Crítico	P3	P2	P1	P1	P1
Muy alto	P3	P2	P1	P1	P1
Alto	P3	P3	P2	P1	P1
Medio	P4	P3	P3	P2	P2
Bajo	P4	P4	P3	P3	P2

A continuación se presentan los tiempos de respuesta máximos ante eventos de seguridad. El **tiempo de respuesta** es el tiempo que se tarda en iniciar los trabajos orientados al análisis y notificación al personal del Área de Sistemas del Ayuntamiento de Cuenca de un determinado evento contado a partir del momento de su registro en el sistema. El cauce de notificación al personal del ayuntamiento se acordará una vez puesto en marcha el sistema.

	Días Laborales	Días Laborales	Sábados, Domingos y Festivos
Prioridad	L-V 9:00 14:00	L-V 14:00 a 9:00	
P1	1 hora	2 horas	2 horas
P2	2 horas	4 horas	4 horas
P3	4 horas	16 horas	16 horas
P4	8 horas	24 horas	24 horas

2.3.- Entregables

El adjudicatario deberá proporcionar los siguientes entregables que deberán ser validados por el Ayuntamiento de Cuenca para su aceptación.

- Manuales y otro material relacionado con la transferencia de conocimientos.
- Informes periódicos de las actuaciones realizadas.
- Documentación de instalación, parametrización y configuración.

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.

No se requiere de dedicación exclusiva del equipo humano adscrito a los diferentes servicios especializados descritos en el presente pliego, siempre y cuando su trabajo habitual consista en prestar servicios equivalentes a otros clientes. Es decir, es admisible que el personal del SOC asociado a este contrato ejerza la misma función con otros clientes, pero no es admisible que se presente como un recurso del SOC un técnico que en su labor diaria no sea realizar este tipo de servicio.

Con carácter general, los equipos de trabajo asignados a la prestación de los servicios solicitados estarán ubicados en los centros de operaciones de la empresa adjudicataria. Independientemente de la posibilidad de comunicación por vía telemática, a efectos operativos y de la gestión del servicio, para las tareas

técnicas que no requieran la presencia obligatoria de la empresa en dependencias del Ayuntamiento de Cuenca, se habilitarán los medios técnicos más adecuados para que puedan realizarse en dependencias de la empresa adjudicataria.

4.- Transferencia Tecnológica

Durante la ejecución de los trabajos derivados del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por el Ayuntamiento de Cuenca la información y documentación que éstas soliciten para disponer de un pleno conocimiento técnico de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas técnicos que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

5.- Devolución del Servicio

Toda la información en posesión del adjudicatario como resultado de la relación con este contrato e independientemente de su naturaleza, deberá de ser devuelta o destruida tras la finalización de la relación contractual, salvo que deban de ser conservados por requerimientos legales o normativos vigentes.

El acuerdo de confidencialidad tendrá validez a partir del momento en que quede firmado por ambas partes, y se extenderá de forma indefinida, a pesar de que haya finalizado la relación contractual.

El adjudicatario estará obligado, previa finalización del plazo de ejecución de los trabajos, a proveer toda la información y documentación necesarias para devolver la responsabilidad del servicio al Ayuntamiento de Cuenca o a quien éste determine, ofreciendo toda la ayuda necesaria en la transmisión del conocimiento relacionado con los servicios que estaba prestando con el fin de permitir una transferencia correcta de los mismos.

Esta transferencia de responsabilidades tendrá que planificarse y llevarse a cabo de manera que evite cualquier problema en la prestación de los servicios. La transferencia deberá contemplar tanto el conocimiento tácito como el explícito, por lo que deberán de contemplarse las sesiones de transferencia de conocimiento necesarias entre el adjudicatario y el equipo destinatario, así como la disponibilidad por parte del adjudicatario para prestar soporte telefónico ante dudas durante el periodo de traspaso y al menos durante un periodo no inferior a UN MES inmediatamente posterior a dicho traspaso.

El adjudicatario deberá aportar en este caso un plan para dicha transferencia, que incluirá al menos: relación de la documentación y del conocimiento a transferir, tanto a nivel técnico como funcional, requerimientos que deberá cumplir el receptor (perfil, conocimientos previos, etc.), estrategia o método recomendado para el traspaso (paralelo, workshops, equipos mixtos, etc.), y marco temporal para el traspaso.

Cuenca, en fecha de firma electrónica