

MEMORIA JUSTIFICATIVA DE LA NECESIDAD DE UNA SOLUCIÓN CONCRETA EN EL EXPEDIENTE ACR-034-2025

“Vigilancia Digital basado en - Recorded Future-”



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1036711525965542862934**

Esta memoria justifica la decisión de especificar una solución tecnológica concreta, el software RECORDED FUTURE (o un equivalente), para la renovación de las licencias de ciberseguridad actuales.

El expediente ACR-034-2025 tiene como objetivo contratar el suministro, mantenimiento y actualización de este software, que es utilizado por el personal técnico de diversas Entidades Locales de la Comunidad de Madrid.

Esta elección particular se realiza de forma excepcional a la habitual neutralidad tecnológica de la Agencia de Ciberseguridad de la Comunidad de Madrid, dada la naturaleza crítica de la plataforma de inteligencia basada en la nube que se requiere para garantizar la seguridad de la red.

La tecnología de la infraestructura actual condiciona las nuevas adquisiciones ya que, de ser sustituidos por otros, previsiblemente supondrían un esfuerzo y unos sobrecostes desproporcionados para la Agencia.

1.-ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD

En la actualidad, la Agencia provee de un servicio de Vigilancia Digital a las Entidades Locales de menos de 20.000 habitantes (en adelante EELL<20K), basado en una plataforma de inteligencia en la nube, el software Recorded Future en régimen de cesión de derecho de uso.

Es por ello que, ante la finalización del periodo de vigencia de las precitadas licencias y con la finalidad de poder continuar dando servicio de seguridad a estas EELL<20K, se hace necesario disponer de las precitadas licencias del software Recorded Future o equivalente.

La continuidad de las licencias del software Recorded Future es un requisito crítico para el mantenimiento de la postura de ciberseguridad de las entidades locales.

La interrupción de este servicio generaría una brecha de seguridad inmediata, comprometiendo la integridad, disponibilidad y confidencialidad de los datos. Esta situación no solo paralizaría servicios esenciales, sino que también expondría a las entidades a un incumplimiento de sus obligaciones legales en materia de protección de datos, lo que podría derivar en graves sanciones regulatorias, perjuicios económicos y un daño irreparable a su reputación.

La caducidad de las licencias representa una vulnerabilidad conocida y de alto riesgo en ciberseguridad. Sin las actualizaciones de seguridad, los parches y el soporte técnico que garantizan estas licencias, el software se volvería obsoleto y vulnerable a ciberataques, comprometiendo todo el entorno digital de las entidades.



Por lo tanto, la renovación de las licencias del software Recorded Future no es una mera cuestión operativa, sino una medida estratégica indispensable para la mitigación de riesgos, la garantía de la continuidad del servicio y el cumplimiento normativo, elementos fundamentales para la seguridad de la información en las entidades públicas.

La arquitectura de seguridad actual representa una inversión significativa en tiempo y recursos, ya que fue construida y optimizada específicamente para el software Recorded Future.

Inversión y Riesgos de Migración

El cambio a un producto alternativo no es una simple sustitución, sino que implica una migración compleja y costosa. Esto incluiría la reestructuración de la infraestructura, la reconfiguración de datos y la capacitación del personal. Estos costes son directos y muy elevados, además de generar un alto riesgo de interrupciones del servicio, pérdida de datos o fallos de seguridad imprevistos durante la transición.

Integración y Postura de Seguridad

Nuestra arquitectura actual se integra de manera profunda con las funcionalidades específicas del producto Recorded Future (APIs, protocolos, etc.). Una solución alternativa podría carecer de estas características, forzando la reconfiguración o el reemplazo de otros componentes esenciales.

Además, el uso del software actual nos permite gestionar un conjunto de riesgos conocidos. Contamos con procedimientos establecidos para monitorear vulnerabilidades y responder a incidentes. Un nuevo producto, por el contrario, introduciría riesgos desconocidos y una curva de aprendizaje que podría comprometer nuestra postura de seguridad, haciendo que la transición sea una opción de alto riesgo.

En resumen, la justificación no se basa en que el producto alternativo sea peor, sino en el alto coste y el riesgo inherente al cambio. La renovación de las licencias actuales es la opción más segura, estable y económicamente viable para mantener la continuidad del negocio y el nivel de protección en ciberseguridad que ya se ha logrado con la arquitectura existente. Es una decisión estratégica que prioriza la estabilidad y la mitigación de riesgos sobre la adopción de una tecnología potencialmente nueva.

Asimismo, hay que indicar que sólo se considerarán equivalentes las soluciones que garanticen la compatibilidad e interoperabilidad con todos los elementos físicos y lógicos de los sistemas, sin que se deba hacer ninguna instalación ni modificación adicional sobre los mismos, ni que suponga desembolsos adicionales o costes de recursos humanos.



2. DESCRIPCIÓN FUNCIONAL DE LOS SUMINISTROS A ADQUIRIR

Se requiere la adquisición de una solución de ciberseguridad, una solución de gestión de exposición basada en la implementación de una plataforma de ciberinteligencia en modalidad SaaS (Software como Servicio) y se requiere que cumpla con las siguientes características como mínimo para cubrir las necesidades de la Agencia de ciberseguridad de la comunidad de Madrid

- **Recopilar y procesar información proveniente de diversas fuentes públicas y privadas.**
- La plataforma debe **integrar capacidades avanzadas de análisis y procesamiento de datos**, permitiendo interpretar la información de forma clara y comprensible.
- Su objetivo principal será **facilitar la toma de decisiones estratégicas y operativas**, optimizando la gestión de la seguridad y fortaleciendo la capacidad de respuesta frente a amenazas y riesgos emergentes en el ámbito de la ciberseguridad.
- Proveer **Servicio Workforce 25k** ofrece a las organizaciones la posibilidad de identificar y gestionar las amenazas relacionadas con las identidades de sus empleados, incluyendo información sobre riesgos como credenciales comprometidas, fugas de datos y actividad maliciosa
- Proporcionar un servicio **de Inteligencia de Terceros**, ofrece información y análisis sobre amenazas cibernéticas que pueden afectar a las organizaciones. Esto incluye la detección de patrones de ataque utilizados por hackers y recomendaciones para implementar medidas de seguridad que protejan contra futuros incidentes.
- **Proveer un servicio Take Down** que permitirá eliminar rápidamente contenido malicioso o fraudulento que abusa de su marca, como sitios web falsos o contenido en redes sociales. Funciona detectando incidentes relacionados con la marca a través de inteligencia de amenazas y solicitando la eliminación de estos contenidos a través de un centro de operaciones que trabaja las 24 horas.

Se trata con este expediente de adquirir las licencias necesarias para dar continuidad a los servicios anteriormente descritos durante 24 meses.



3. DETALLE DE LA NECESIDAD A CUBRIR

El detalle de las licencias y cantidad necesaria se indica en la siguiente tabla

Part Number	Programa	Periodo de vigencia del licenciamiento	Cantidad
FOUNDATION	Recorded Future Foundation	24 meses	1
ID-WF-25K	Identity Intelligence - Workforce 25k	24 meses	1
TPI-100	Third-Party Intelligence – 100 Companies	24 meses	1
TKD-25	Takedown Services (25)	24 meses	1

4. MOTIVACIONES PARA ADQUIRIR EL SUMINISTRO A UN FABRICANTE CONCRETO

Adquirir suministros con características técnicas diferentes daría lugar a incompatibilidades o dificultades técnicas de uso y mantenimiento y/o costes (de capacitación, pruebas de compatibilidad, elementos complementarios, mantenimiento, etc.) que resultarían desproporcionados para esta Agencia.

Es por todo ello que a continuación se detallan los condicionantes tecnológicos que motivan la contratación de la solución en ciberseguridad RECORDED FUTURE o equivalente:



- **Inversión y Estabilidad de la Arquitectura Existente**

- La arquitectura de seguridad actual se ha construido y optimizado para funcionar de manera nativa con Recorded Future. Cambiar de producto implicaría una migración costosa y compleja, con un alto riesgo de interrupciones del servicio, pérdida de datos y vulnerabilidades de seguridad imprevistas. La renovación garantiza la continuidad, estabilidad y el retorno de la inversión ya realizada.

- **Gestión de Riesgos y Cumplimiento Normativo**

- Al mantener el producto actual, se garantiza que la infraestructura de seguridad siga recibiendo las actualizaciones, parches y el soporte técnico esenciales para defenderse de las amenazas cibernéticas más recientes. Esto permite una mitigación de riesgos proactiva y asegura el cumplimiento continuo de las obligaciones legales y normativas en materia de protección de datos, evitando sanciones y daños a la reputación.

- **Conocimiento y Eficiencia del Equipo**

- El personal técnico ya posee un conocimiento profundo y especializado en el manejo, la configuración y el mantenimiento de Recorded Future. Esta experiencia asegura una operación eficiente, minimiza los errores humanos y permite una respuesta rápida y efectiva ante cualquier incidente de seguridad. La adopción de un nuevo producto requeriría una curva de aprendizaje considerable, lo que podría comprometer la eficiencia y la seguridad durante la transición, además de evitar la repetición de la parametrización realizada, así como de la configuración específica para las necesidades de los servicios prestados por la Agencia.

- **Coherencia y Complejidad Tecnológica**

- La integración de Recorded Future con otros sistemas de seguridad de la red ya está establecida. Un cambio de producto podría romper estas integraciones, requiriendo una reconfiguración completa de la red y la posible sustitución de otros componentes. Mantener la solución actual simplifica la infraestructura tecnológica, reduce la complejidad de la gestión y asegura que todos los elementos de seguridad trabajen de forma coherente.
- Por otro lado, la misma solución, ya implantada en otros organismos (Salud digital) dependientes de la Consejería de Digitalización a la que también pertenece la Agencia de Ciberseguridad, garantiza homogeneidad tecnológica, alineación de estándares y reutilización de configuraciones, lo que reduce la heterogeneidad y los costes de coordinación entre áreas. Esto permite compartir librerías de casos de uso, taxonomías, conectores y



procedimientos, acortando tiempos de despliegue y facilitando la operación conjunta.

• **Análisis de Costes y Viabilidad Económica**

La decisión de renovar las licencias de Recorded Future se basa en un análisis de costes que va más allá del precio de la licencia, considerando el coste total de propiedad y la gestión de riesgos financieros.

- **Minimización de Costes de Migración e Implementación:** La migración a un producto alternativo implicaría una inversión considerable y no presupuestada en recursos humanos y tecnológicos. Los costes directos de reestructuración de la infraestructura, reconfiguración de datos y validación de la nueva plataforma serían muy elevados. Además, el riesgo de inactividad del servicio durante la transición tiene un impacto financiero directo e inaceptable en nuestra operatividad.
- **Ahorro en Capacitación y Formación:** Nuestros equipos ya están formados y certificados en el uso y mantenimiento de Recorded Future. Cambiar de plataforma requeriría una nueva inversión significativa en capacitación del personal, además de la pérdida de productividad inherente a la curva de aprendizaje de una tecnología desconocida. Mantener la solución actual evita estos gastos y asegura la máxima eficiencia operativa desde el primer día.
- **Mitigación de Riesgos Financieros:** La renovación es una medida de mitigación de riesgos financieros. La interrupción del servicio o un fallo de seguridad derivado de la obsolescencia tecnológica no solo afectaría a los servicios críticos, sino que también expondría a la organización a sanciones regulatorias y a una potencial pérdida de ingresos. Estos riesgos financieros superan con creces el coste de la renovación de las licencias.
- **Optimización de la Inversión Existente:** La renovación de Recorded Future permite maximizar el retorno de la inversión ya realizada en la arquitectura de seguridad. Al no tener que desechar la infraestructura y las integraciones actuales, se optimizan los recursos financieros y se garantiza que los sistemas funcionen de manera coherente y eficiente, sin necesidad de adquirir nuevo hardware o software para asegurar la compatibilidad.

En definitiva, se trata de una tecnología ya homologada en nuestra organización, se han normalizado los procesos de administración, desarrollo, despliegue, operación y explotación. La interoperabilidad de esta tecnología con otros sistemas está ya probada, habiéndose realizado la homologación con todos los servicios relacionados. Una nueva tecnología requeriría repetir de nuevo dichos trabajos, con el coste y dedicación correspondientes.



El Consejero Delegado de la Agencia de Ciberseguridad

Fdo.: Alejandro Las Heras Vázquez



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1036711525965542862934**