

MEMORIA JUSTIFICATIVA DE LA NECESIDAD DE UNA SOLUCIÓN CONCRETA EN EL EXPEDIENTE ACR-035-2025

**Licenciamiento de solución de arquitectura de
ciberseguridad en la nube “Secure Access Service
Edge – SASE”**



La autenticidad de este documento se puede comprobar en
<https://gestion.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055373893065017742391**

MEMORIA JUSTIFICATIVA DE LA NECESIDAD CONCRETA

Esta memoria recoge las razones por las que en el expediente ACR-035-2025 para la contratación del suministro, mantenimiento y derecho de actualización del software SASE - Zscaler para la renovación de las licencias del software de ciberseguridad utilizado actualmente por el personal técnico de distintas Entidades locales de la Comunidad de Madrid, se requiere una solución tecnológica determinada como es el software SASE-Zscaler - ZIA y ZPA -, haciendo una excepción a la habitual neutralidad tecnológica de la Agencia de Ciberseguridad de la Comunidad de Madrid (en adelante, Agencia).

La tecnología de la infraestructura actual condiciona las nuevas adquisiciones ya que, de ser sustituidos por otros, previsiblemente supondrían un esfuerzo y unos sobrecostos desproporcionados para la Agencia. Así mismo, técnicamente, no se podría asegurar que el servicio pudiera seguir manteniéndose en los niveles actualmente exigidos en seguridad.

1. ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD

En la actualidad, la Agencia dispone de licencias del software Zscaler (ZIA y ZPA) en régimen de cesión de derecho de uso para dar cobertura de seguridad a diferentes Entidades Locales de menos de 20.000 habitantes (en adelante EELL<20K)

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 Zscaler.

La interrupción de licencias en un sistema como el descrito genera una brecha de seguridad que podría afectar a la integridad, disponibilidad y confidencialidad de los datos. Al dejar de funcionar los servicios críticos, la empresa incumple su obligación legal de proteger la información, exponiéndose a sanciones, pérdidas económicas y daños a su reputación.

El final del ciclo de vida de un producto o licencia es una vulnerabilidad conocida en ciberseguridad. Cuando una licencia expira o deja de ser soportada, deja de recibir actualizaciones de seguridad, parches y soporte técnico, lo que convierte al software en un objetivo fácil para los ciberataques.



Por lo tanto, la renovación de estas licencias no es solo una cuestión operativa, sino una medida esencial de ciberseguridad para mitigar los riesgos, asegurar la continuidad del negocio y garantizar el cumplimiento de las normativas de protección de datos.

La arquitectura actual se construyó, probó y optimizó específicamente para funcionar con las licencias y el software existente. Esto representa una inversión considerable en tiempo, dinero y recursos humanos. Cambiar a un producto alternativo no es simplemente "instalar un nuevo software". Implica una migración completa de datos y configuraciones, reentrenamiento del personal, y una posible reestructuración de la infraestructura para asegurar la compatibilidad. Estos costes son directos y muy elevados. Durante la migración, existe un alto riesgo de interrupciones del servicio, pérdida de datos o fallos de seguridad no previstos. Esto podría comprometer la disponibilidad y la integridad de los sistemas críticos, un aspecto fundamental de la ciberseguridad. La arquitectura existente probablemente depende de funcionalidades específicas del producto actual. Sus API, protocolos de comunicación y modos de integración con otros sistemas de la empresa (como SIEM, IAM, etc.) son únicos. Un producto alternativo podría no tener las mismas características, lo que obligaría a reconfigurar o incluso reemplazar otros componentes de la arquitectura.

Al mantener el producto actual, la empresa se enfrenta a un conjunto de riesgos conocidos y gestionados. Se tienen procedimientos establecidos para aplicar parches, monitorear vulnerabilidades y responder a incidentes. Un nuevo producto, por muy bueno que sea, trae consigo un nuevo conjunto de riesgos desconocidos y vulnerabilidades que aún no han sido plenamente identificadas o gestionadas por la empresa.

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, 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 basada en la nube para la inspección, análisis y gestión de tráfico y datos provenientes de diversas fuentes, tanto públicas como privadas, para la actualización y crecimiento vegetativo sobre la plataforma Zscaler durante 3 años. El objetivo es optimizar la gestión de la seguridad, garantizar el acceso seguro a aplicaciones y fortalecer la capacidad de respuesta frente a amenazas emergentes mediante un enfoque Zero Trust y tecnologías avanzadas como Secure Web Gateway, Cloud Firewall y ZTNA.

Se trata con este expediente de adquirir las licencias necesarias para dar continuidad a los servicios anteriormente descritos y que deberán cumplir, al menos, con los siguientes requisitos funcionales:

Seguridad y Acceso a la Nube:

Proporcionar un acceso seguro a internet y a las aplicaciones para todos los usuarios y dispositivos, independientemente de su ubicación.

Utilizar un enfoque de Confianza Cero (Zero Trust) para proteger a los usuarios y las aplicaciones, eliminando el concepto de perímetro de seguridad tradicional.

Acceso a la Red con Confianza Cero (ZTNA):

Ofrecer acceso seguro y directo a aplicaciones y servicios privados internos sin la necesidad de una VPN tradicional.

Permitir a los usuarios conectarse a aplicaciones específicas sin exponer toda la red corporativa, reduciendo así la superficie de ataque.

Protección Avanzada contra Ciberamenazas:

Inspeccionar el tráfico en tiempo real para detectar y bloquear actividad maliciosa.

Utilizar tecnologías avanzadas (como la detección impulsada por IA y el sandboxing) para identificar y neutralizar amenazas como el malware, el ransomware y los ataques de phishing.

Gestión de Red y Conectividad:

Ofrecer una solución de red que reemplace las VPNs y el enrutamiento complejo con una arquitectura directa a la nube.

Garantizar un acceso seguro y fiable a las aplicaciones (tanto en la nube como en las instalaciones) para sucursales, campus y otros entornos distribuidos.

Minimizar el movimiento lateral de amenazas y el riesgo de ransomware al simplificar la infraestructura de red y eliminar la necesidad de puertos expuestos.



3. DETALLE DE LA NECESIDAD A CUBRIR

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

Referencia	Programa	CANTIDAD
ZS-ESS-PLATFORM o equivalente	Zscaler Essentials Platform o equivalente	3.000
ZS-ZPA-PLATFORM o equivalente	Zscaler Private Access Platform o equivalente	3.000
ZS-ZPA-2 o equivalente	Zscaler Private Access o equivalente	3.000
ZS-CPT-1 o equivalente	Zscaler Inline Cyber Threat Protection o equivalente	3.000
ZT- SDWAN – 400 o equivalente	Zero Trust SD-WAN: ZT 400 o equivalente	80
ZCES-SUP-PREM o equivalente	PREMIUM SUPPORT ADVANCE o equivalente	1



La autenticidad de este documento se puede comprobar en
<https://gestiona.comunidad.madrid/csv>
mediante el siguiente código seguro de verificación: **1055373893065017742391**

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 SASE Zscaler o equivalente:

- **Requisitos de Integración y Compatibilidad**
 - La plataforma de servicios SASE (como Zscaler o un equivalente) debe integrarse de forma nativa con nuestra arquitectura de seguridad existente. Esta integración es indispensable para asegurar una protección exhaustiva de los datos en todos los procesos críticos de la Agencia y para complementar eficazmente los demás sistemas de seguridad de la información ya implementados en las EELL<20K.
- **Experiencia y Capacitación del Equipo**
 - Nuestros equipos técnicos y de seguridad ya poseen un profundo conocimiento y experiencia en la gestión de la plataforma SASE (Zscaler o un equivalente). Esta especialización garantiza una implementación y operación eficientes, reduce los riesgos asociados a la curva de aprendizaje de un nuevo producto y asegura una respuesta más rápida y efectiva ante posibles incidentes de seguridad. La continuidad en el uso de una tecnología familiar optimiza los procesos de seguridad y minimiza el riesgo de errores humanos en la configuración.
- **Impacto en la Continuidad y Calidad del Servicio**
 - La discontinuidad de las licencias o una migración a una plataforma SASE alternativa conlleva un riesgo directo y significativo para la continuidad del negocio. Nuestros servicios más críticos, especialmente en la atención al ciudadano, dependen de la disponibilidad y seguridad que proporciona la plataforma actual.
 - Cualquier interrupción o fallo en la transición podría provocar que estos servicios dejen de prestarse, afectando no solo a nuestras operaciones internas, sino también a la calidad del servicio que se ofrece a los clientes. Esto podría generar una pérdida de confianza y tener graves consecuencias legales y reputacionales para la organización. Mantener la plataforma actual es esencial para garantizar un servicio estable y fiable.



- **Análisis de Costes y Viabilidad Económica**

- La renovación del producto actual es la opción más viable económicamente a largo plazo. Cambiar a una solución alternativa, aunque ofrezca un coste de licencia potencialmente más bajo, implicaría incurrir en una serie de costes ocultos y directos que superan cualquier ahorro inicial como:
 - **Costes de Migración e Implementación:** Se requeriría una inversión considerable en tiempo y recursos para planificar, ejecutar y probar la migración de la arquitectura de seguridad, con el riesgo inherente de interrupciones del servicio.
 - **Costes de Capacitación:** Sería necesario invertir en la formación y certificación de los equipos de TI y seguridad en la nueva plataforma, lo que generaría una pérdida de productividad durante el periodo de adaptación.
 - **Costes de Oportunidad y Riesgo:** El mayor riesgo financiero reside en el impacto negativo sobre la continuidad del negocio y la potencial pérdida de ingresos o sanciones derivadas de fallos de seguridad durante la transición.
- 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: **1055373893065017742391**