# Solicitud de Propuesta: Plataformas de Borde de Servicio de Acceso Seguro (SASE)

## Índice



## 1. 1. Introducción y antecedentes

[Nombre de la empresa] busca propuestas para una plataforma integral de Secure Access Service Edge (SASE) para modernizar nuestra infraestructura de red y seguridad. Esta RFP describe nuestros requisitos para una solución nativa de la nube que converge la conectividad de red y los servicios de seguridad para apoyar nuestra fuerza de trabajo distribuida y las iniciativas de la nube primero.

### Antecedentes de la organización

- [Describa su empresa/organización]
- [Requisitos industriales y reglamentarios]
- [Tamaño de la organización e infraestructura informática]

### Entorno actual

- [Arquitectura actual de red y seguridad]
-

- [Número de usuarios y ubicaciones]

### Objetivos del proyecto

- Implantación de una arquitectura SASE unificada y nativa de la nube
- Mejora de la seguridad mediante servicios integrados
- Optimización del rendimiento de la red y de la experiencia del usuario
- Gestión y operaciones racionalizadas

## 2. Objetivos del proyecto

1. Implantar una plataforma SASE completa que integre:
    - Redes de área extensa definidas por software (SD-WAN)
    - Componentes de Security Service Edge (SSE)
    - Acceso a la red de confianza cero (ZTNA)
    - Servicios de seguridad en la nube
2. Conseguir los siguientes resultados:
    - Infraestructura unificada de seguridad y redes
    - Mayor visibilidad y control
    - Mejora de la eficacia operativa
    - Reducción del coste total de propiedad
    - Arquitectura escalable nativa en la nube

## 3. 3. Alcance del trabajo

### Componentes necesarios

1. Capacidades de SD-WAN
    - Optimización de la red
    - Enrutamiento sensible a las aplicaciones
    - Gestión de enlaces WAN

- Controles QoS

2. Servicio de seguridad Edge (SSE)
    - Pasarela web segura (SWG)
    - Agente de seguridad de acceso a la nube (CASB)
    - Acceso a la red de confianza cero (ZTNA)
    - Cortafuegos como servicio (FWaaS)
3. Funciones de seguridad avanzadas
    - Prevención de pérdida de datos (DLP)
    - Protección avanzada contra amenazas
    - Análisis del comportamiento de usuarios y entidades
    - Inteligencia integrada sobre amenazas
4. Gestión y análisis
    - Consola de gestión unificada
    - Control en tiempo real
    - Análisis avanzados
    - Respuesta automatizada a incidentes

## Fases de aplicación

1. Planificación y diseño
    - Evaluación de la arquitectura
    - Desarrollo de la estrategia de migración
    - Diseño del marco político
    - Evaluación de la infraestructura actual de red y seguridad
    - Formación y planificación de la gestión del cambio para el personal informático y los usuarios finales

2. Despliegue piloto
    - Aplicación inicial
    - Pruebas y validación
    - Establecimiento de una base de referencia
    - Ejecución de pruebas de concepto (PoC), incluyendo:
        - Objetivos y criterios de éxito claros
        - Pruebas de casos de uso clave
        - Parámetros de rendimiento y escenarios de seguridad
        - Pruebas de integración necesarias
        - Métricas de evaluación y requisitos de información
3. Despliegue completo
    - Implantación gradual
    - Migración de usuarios
    - Integración con los sistemas existentes
4. Optimización
    - Ajuste del rendimiento
    - Perfeccionamiento de las políticas
    - Optimización de la experiencia del usuario

## 4. 4. Requisitos técnicos

### Capacidades de red

1. Características de SD-WAN
    - Enrutamiento sensible a las aplicaciones
    - Selección dinámica de rutas
    - Gestión de la calidad del servicio y del ancho de banda

- Agregación de enlaces y conmutación por error
- Conformación y priorización del tráfico

## 5. 5. Requisitos funcionales

### A. Requisitos funcionales básicos

#### 5.1 Arquitectura nativa de la nube

*Consejo: Una arquitectura nativa de la nube es fundamental para una implementación exitosa de SASE. Busque soluciones que demuestren verdaderos principios de diseño cloud-first, con una arquitectura basada en microservicios que permita escalabilidad, flexibilidad y operaciones resistentes. Considere cómo la arquitectura soporta el despliegue distribuido y mantiene un rendimiento consistente en diferentes entornos de nube.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Arquitectura nativa de la nube | Diseño cloud-first con arquitectura de microservicios | | |
| | Capacidades de despliegue basadas en contenedores | | |
| | Autoescalado y gestión elástica de recursos | | |
| | Arquitectura multiusuario | | |
| | Integración nativa de proveedores de servicios en la nube | | |

#### 5.2 Capacidades SD-WAN integradas

*Consejo: La integración eficaz de SD-WAN es crucial para optimizar el rendimiento de la red y garantizar una conectividad fiable en ubicaciones distribuidas. Céntrese en soluciones que ofrezcan funciones completas de optimización de la WAN y capacidades de enrutamiento inteligente del tráfico, al tiempo que mantienen un rendimiento constante de las aplicaciones.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Integración SD-WAN | Capacidades de enrutamiento sensibles a las aplicaciones | | |
| | Optimización y selección dinámica de rutas | | |
| | Equilibrio de carga y agregación de enlaces WAN | | |
| | Controles de calidad de servicio (QoS) | | |
| | Gestión y optimización del ancho de banda | | |

### 5.3 Servicios integrales de seguridad

*Consejo: Los servicios de seguridad constituyen la columna vertebral de la arquitectura SASE. Evalúe las soluciones en función de su capacidad para proporcionar controles de seguridad integrados y en la nube que protejan todos los extremos de la red, manteniendo la sencillez en la gestión y la implantación.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Servicios de seguridad | Funciones de cortafuegos de nueva generación | | |
| | Funciones avanzadas de prevención de amenazas | | |
| | Funciones de prevención de pérdida de datos (DLP) | | |
| | Acceso a la red de confianza cero | | |
| | Servicios de pasarela web segura | | |

### 5.4 Interfaz de gestión unificada

*Consejo: Una interfaz de gestión centralizada es esencial para la eficacia de las operaciones de SASE. Busque soluciones que ofrezcan un control intuitivo y exhaustivo a través de un único panel de control que permita la gestión unificada de políticas, la supervisión y la generación de informes, al tiempo que se adapte a diferentes roles administrativos y niveles de acceso.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Interfaz de gestión | Consola única para todas las funciones de SASE | | |
| | Gestión del control de acceso basado en funciones | | |
| | Cuadros de mando e informes personalizables | | |
| | Gestión integrada de políticas | | |
| | Capacidad de configuración en tiempo real | | |

### 5.5 Aplicación de la política

*Consejo: La aplicación coherente de políticas en todos los bordes de la red y funciones de seguridad es fundamental para mantener la postura de seguridad. Evalúe las soluciones en función de su capacidad para aplicar las políticas granulares de manera uniforme, al tiempo que admiten ajustes dinámicos basados en el contexto y el riesgo.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Aplicación de la política | Creación y control granular de políticas | | |
| | Gestión de políticas basadas en usuarios y grupos | | |
| | Aplicación de la política de localización | | |
| | Aplicación de normas específicas de la aplicación | | |
| | Implantación automatizada de políticas | | |

### 5.6 Optimización del tráfico

*Consejo: Las funciones de optimización del tráfico repercuten directamente en la experiencia del usuario y el rendimiento de las aplicaciones. Céntrese en soluciones que ofrezcan funciones de optimización integrales al tiempo que mantienen la seguridad y la visibilidad en todos los flujos de tráfico.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Optimización del tráfico | Optimización del tráfico WAN | | |
| | Aceleración del rendimiento de las aplicaciones | | |
| | Controles de asignación de ancho de banda | | |
| | Mecanismos de priorización del tráfico | | |
| | Capacidades de implementación de QoS | | |

### 5.7 Escalabilidad

*Consejo: La escalabilidad garantiza que su solución SASE pueda crecer con su organización. Considere las capacidades de escalado horizontal y vertical, junto con la capacidad de mantener el rendimiento a medida que se amplía el despliegue.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Escalabilidad | Soporte de escalado horizontal | | |
| | Gestión de recursos elásticos | | |
| | Optimización del rendimiento a escala | | |
| | Planificación automatizada de la capacidad | | |
| | Equilibrio dinámico de la carga | | |

### 5.8 Capacidades de integración

*Consejo: Las capacidades de integración determinan lo bien que funciona la solución SASE con su infraestructura existente. Evalúe la amplitud y profundidad de las opciones de integración, centrándose en las API y los conectores preconstruidos para sistemas empresariales comunes.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Integración | Disponibilidad y documentación de la API | | |
| | Integración de sistemas SIEM | | |

| | | | |
|---|---|---|---|
| | Conectividad de proveedores de identidad | | |
| | Integración de herramientas de seguridad de terceros | | |
| | Capacidades de integración personalizadas | | |

### 5.9 Protección avanzada contra amenazas

*Consejo: La protección avanzada contra amenazas es crucial en el panorama actual de amenazas en evolución. Busque soluciones que combinen varios métodos de detección con funciones de respuesta automatizada para ofrecer una protección completa frente a ataques sofisticados.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Protección frente a amenazas | Prevención de amenazas de día cero | | |
| | Funciones avanzadas de sandboxing | | |
| | Integración de inteligencia sobre amenazas | | |
| | Funciones de análisis del comportamiento | | |
| | Respuesta automatizada a las amenazas | | |

### 5.10 Gestión de identidades y accesos

*Consejo: El control de acceso basado en la identidad es fundamental para la seguridad de confianza cero. Evalúe las soluciones en función de su capacidad para integrarse con los sistemas de identidad existentes y, al mismo tiempo, ofrecer sólidas funciones de autenticación y autorización.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| IAM | Autenticación multifactor | | |
| | Inicio de sesión único | | |
| | Integración de servicios de directorio | | |

| | | | |
|---|---|---|---|
| | Gestión de accesos privilegiados | | |
| | Mecanismos de verificación de identidad | | |

### 5.11 Supervisión y análisis en tiempo real

*Consejo: Una supervisión y un análisis eficaces proporcionan visibilidad de la seguridad y el rendimiento. Céntrese en soluciones que ofrezcan funciones integrales de supervisión en tiempo real con información práctica e informes personalizables.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Supervisión y análisis | Control del rendimiento en tiempo real | | |
| | Análisis de eventos de seguridad | | |
| | Seguimiento de la experiencia del usuario | | |
| | Análisis del rendimiento de la red | | |
| | Herramientas de elaboración de informes personalizables | | |

### 5.12 Soporte multi-nube

*Consejo: La compatibilidad con varias nubes es esencial para las arquitecturas distribuidas modernas. Evalúe las soluciones en función de su capacidad para ofrecer una seguridad y conectividad coherentes entre distintos proveedores de nubes, manteniendo al mismo tiempo una gestión unificada.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Nube múltiple | Conectividad entre nubes | | |
| | Seguridad de nube a nube | | |
| | Seguridad de acceso a la nube | | |
| | Protección de cargas de trabajo en la nube | | |
| | Herramientas de gestión multinube | | |

### 5.13 Soporte Edge Computing

*Consejo: La informática de borde permite un procesamiento más cercano a las fuentes de datos. Busque soluciones que puedan ampliar la seguridad y las capacidades de red a ubicaciones periféricas manteniendo el control centralizado.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Computación de borde | Despliegue de servicios Edge | | |
| | Apoyo al tratamiento local de datos | | |
| | Controles de seguridad periféricos | | |
| | Optimización del rendimiento de los bordes | | |
| | Características de la informática distribuida | | |

### 5.14 Respuesta automatizada a incidentes

*Consejo: Las capacidades automatizadas de respuesta a incidentes reducen el tiempo medio de respuesta y recuperación ante incidentes de seguridad. Céntrese en soluciones que proporcionen una automatización completa, manteniendo al mismo tiempo una supervisión humana adecuada.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Respuesta a incidentes | Mitigación automatizada de amenazas | | |
| | Automatización del flujo de trabajo de incidencias | | |
| | Orquestación de la respuesta | | |
| | Procedimientos automatizados de recuperación | | |
| | Herramientas de análisis posterior al incidente | | |

### 5.15 Gestión del cumplimiento

*Consejo: Las funciones de gestión de la conformidad ayudan a mantener el cumplimiento de la normativa. Evalúe las soluciones en función de su capacidad para aplicar las políticas de cumplimiento y generar la documentación y los informes necesarios.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Conformidad | Herramientas de control del cumplimiento | | |
| | Funciones de información reglamentaria | | |
| | Mantenimiento de registros de auditoría | | |
| | Comprobación del cumplimiento de las políticas | | |
| | Cuadro de mandos de cumplimiento de la normativa | | |

## B. Requisitos de la IA y el aprendizaje automático

### 5.16 Seguridad basada en IA

*Consejo: La seguridad basada en IA mejora las capacidades de detección y respuesta ante amenazas. Busque soluciones que aprovechen eficazmente la IA y ofrezcan transparencia en sus procesos de toma de decisiones.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Seguridad AI | Detección de amenazas basada en IA | | |
| | Respuestas de seguridad automatizadas | | |
| | Evaluación de riesgos basada en IA | | |
| | Análisis de aprendizaje automático | | |
| | Análisis de patrones de comportamiento | | |

### 5.17 Integración de la IA Generativa

*Consejo: Las capacidades de IA generativa mejoran los procesos de automatización y toma de decisiones. Céntrese en soluciones que aprovechen la IA generativa para*

*mejorar la configuración, la resolución de problemas y la gestión de directivas, manteniendo al mismo tiempo la seguridad y la precisión.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| IA Generativa | Generación de políticas basadas en IA | | |
| | Asistencia a la configuración automatizada | | |
| | Creación inteligente de documentación | | |
| | Solución de problemas asistida por IA | | |
| | Capacidad de procesamiento del lenguaje natural | | |

### 5.18 Gestión de redes asistida por IA

*Consejo: La gestión de redes asistida por IA mejora la eficiencia operativa y el rendimiento de la red. Evalúe las soluciones en función de su capacidad para automatizar tareas rutinarias y ofrecer recomendaciones de optimización inteligentes.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Gestión de redes de IA | Optimización automatizada de la red | | |
| | Solución inteligente de problemas | | |
| | Predicción de resultados | | |
| | Gestión inteligente de la configuración | | |
| | Capacidades de automatización de redes | | |

### 5.19 Gestión Autónoma de la Experiencia Digital (ADEM)

*Consejo: ADEM garantiza una experiencia de usuario óptima mediante la supervisión y optimización automatizadas. Busque soluciones que ofrezcan una visibilidad completa de la experiencia del usuario y funciones de corrección automatizadas.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|

| | | | |
|---|---|---|---|
| ADEM | Seguimiento de la experiencia en tiempo real | | |
| | Seguimiento del rendimiento de las aplicaciones | | |
| | Puntuación de la experiencia del usuario | | |
| | Solución automatizada de problemas | | |
| | Herramientas de optimización de la experiencia | | |

### 5.20 Operaciones de IA (AIOps)

*Consejo: Las capacidades de AIOps agilizan las operaciones de TI a través de la automatización inteligente. Céntrese en soluciones que combinen eficazmente datos operativos con IA para mejorar la eficiencia y reducir la intervención manual.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| AIOps | Tareas operativas automatizadas | | |
| | Funciones de mantenimiento predictivo | | |
| | Optimización de recursos | | |
| | Sistema de alerta inteligente | | |
| | Optimización del rendimiento | | |

### 5.21 Detección mejorada de amenazas con IA

*Consejo: La detección de amenazas mejorada con IA proporciona una identificación más precisa y rápida de las amenazas a la seguridad. Evalúe las soluciones en función de su capacidad de aprovechar la IA para mejorar la detección de amenazas y minimizar los falsos positivos.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Detección de amenazas mediante IA | Análisis avanzado de amenazas | | |
| | Capacidad de reconocimiento de patrones | | |

| | | | |
|---|---|---|---|
| | Detección de anomalías | | |
| | Identificación predictiva de amenazas | | |
| | Análisis de amenazas en tiempo real | | |

### 5.22 Toma de decisiones basada en IA

*Consejo: La toma de decisiones basada en IA mejora los tiempos de respuesta y la precisión. Busque soluciones que ofrezcan decisiones de IA transparentes y explicables, manteniendo al mismo tiempo una supervisión humana adecuada.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Toma de decisiones con IA | Decisiones políticas automatizadas | | |
| | Evaluación inteligente de riesgos | | |
| | Optimización de la asignación de recursos | | |
| | Decisiones basadas en los resultados | | |
| | Auditorías de decisiones | | |

### 5.23 Interfaces de lenguaje natural

*Consejo: Las interfaces de lenguaje natural mejoran la interacción con el usuario y la eficacia de la gestión. Céntrese en soluciones que ofrezcan un procesamiento intuitivo y preciso del lenguaje natural, manteniendo al mismo tiempo los controles de seguridad.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Lenguaje natural | Interpretación de órdenes | | |
| | Consultas en lenguaje natural | | |
| | Interfaz conversacional | | |
| | Soporte multilingüe | | |

| | | | |
|---|---|---|---|
| | Conocimiento del contexto | | |

### 5.24 Capacidades de IA predictiva

*Consejo: La IA predictiva permite una gestión y optimización proactivas. Evalúe las soluciones en función de su capacidad para predecir con precisión las tendencias y los posibles problemas, al tiempo que proporciona información práctica.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| IA predictiva | Predicción de capacidad | | |
| | Previsión de resultados | | |
| | Predicción de amenazas | | |
| | Previsión del uso de recursos | | |
| | Análisis de tendencias | | |

### 5.25 Asignación de relaciones para UEBA

*Consejo: El mapeo de relaciones UEBA proporciona una visión más profunda de los patrones de comportamiento de los usuarios. Busque soluciones que mapeen y analicen las relaciones de forma eficaz, manteniendo al mismo tiempo los requisitos de privacidad y conformidad.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Cartografía UEBA | Análisis del comportamiento de los usuarios | | |
| | Mapeo de relaciones entre entidades | | |
| | Reconocimiento de patrones | | |
| | Correlación de anomalías | | |
| | Análisis del comportamiento | | |

### 5.26 IA explicable para la detección de anomalías

*Consejo: La IA explicable garantiza la transparencia en los procesos de detección de anomalías. Céntrese en soluciones que ofrezcan explicaciones claras de las anomalías detectadas por la IA sin perder precisión en la detección.*

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| IA explicable | Lógica de decisión transparente | | |
| | Funciones de explicación de anomalías | | |
| | Razonamiento de la detección | | |
| | Generación de registros de auditoría | | |
| | Apoyo a la investigación | | |

## 6. 6. Cualificación de los proveedores

### Cualificaciones requeridas

1. Presentación de la empresa
    - Años en el mercado SASE
    - Posición en el mercado
    - Estabilidad financiera
    - Base de clientes
2. Conocimientos técnicos
    - Experiencia en arquitectura SASE
    - Certificaciones de seguridad
    - Capacidades de aplicación
    - Infraestructura de apoyo
3. Cobertura de servicios
    - Presencia mundial
    - Métricas de disponibilidad del servicio

- Cobertura geográfica
- Puntos de presencia

4. Certificaciones y normas
    - Certificaciones de seguridad
    - Certificaciones de conformidad
    - Adaptación a las normas del sector
    - Marcos de buenas prácticas
5. Desarrollo futuro
    - Hoja de ruta del producto
    - Estrategia de innovación
    - Mejoras previstas
    - Asociaciones tecnológicas

## 7. 7. Criterios de evaluación

Las propuestas se evaluarán en función de

1. Capacidad técnica (30%)
    - Completitud de las características
    - Diseño arquitectónico
    - Métricas de rendimiento
    - Capacidades de seguridad
2. Enfoque de aplicación (20%)
    - Metodología de implantación
    - Estrategia de migración
    - Gestión de riesgos
    - Viabilidad temporal

3. Cualificación de los proveedores (20%)
    - Experiencia
    - Referencias
    - Capacidades de apoyo
    - Estabilidad financiera
4. Estructura de costes (30%)
    - Coste total de propiedad
    - Modelo de precios
    - Costes adicionales
    - Relación calidad-precio

## 8. 8. Normas de presentación

Las propuestas deben incluir:

1. Resumen ejecutivo
2. Descripción de la solución técnica
3. Enfoque de aplicación
4. Calendario del proyecto
5. Precios
6. Cualificaciones de la empresa
7. Referencias de clientes
8. Modelo de apoyo
9. Ejemplos de acuerdos de nivel de servicio
10. Documentación adicional
11. Casos prácticos y referencias
    - Ejemplos de aplicación similares

- Implantaciones específicas del sector
- Métricas de éxito
- Testimonios de clientes

## 9. Cronología

- Fecha de publicación de la RFP: [Fecha]
- Preguntas Plazo: [Fecha]
- Fecha límite para la presentación de propuestas: [Fecha]
- Presentaciones de proveedores: [intervalo de fechas]
- Decisión de selección: [Fecha]
- Inicio del proyecto: [Fecha]
- Finalización prevista: [Fecha]

Envíe sus propuestas a [Información de contacto]