# Solicitud de Propuesta: Soluciones de Gestión de Postura de Seguridad SaaS (SSPM)

## Índice



## 1. Introducción

SaaS Security Posture Management (SSPM) es una solución crítica para las organizaciones que dependen de plataformas en la nube para operaciones críticas. El software SSPM protege continuamente las aplicaciones en la nube detectando vulnerabilidades, garantizando el cumplimiento y mitigando los riesgos de robo de datos.

Esta RFP busca propuestas para una solución SSPM que proporcione protección integral para el entorno SaaS de nuestra organización, incluido el control de acceso, la seguridad de los datos, la supervisión del cumplimiento y la evaluación de riesgos.

## 2. Objetivos del proyecto

La solución debe proporcionar:

- Protección integral para el entorno SaaS de la organización
- Control de acceso sólido y medidas de seguridad de los datos

- Control e informes continuos sobre el cumplimiento
- Capacidades integradas de evaluación de riesgos
- Integración perfecta con la infraestructura existente
- Escalabilidad para apoyar el crecimiento de la organización

## 3. Alcance

El ámbito de aplicación abarca:

- Implantación de una solución SSPM integral
- Integración con la infraestructura de seguridad existente
- Configuración y despliegue
- Formación del personal y transferencia de conocimientos
- Asistencia y mantenimiento continuos
- Actualizaciones periódicas y gestión de parches

## 4. 4. Requisitos funcionales

### 4.1 Descubrimiento e inventario de aplicaciones SaaS

***Consejo: Base esencial para SSPM que requiere descubrimiento automatizado y continuo y visibilidad completa de todas las aplicaciones SaaS para prevenir eficazmente la TI en la sombra y mantener el control de la seguridad.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Descubrimiento y catalogación | Detección automática de todas las aplicaciones SaaS | | |
| | Catalogación y actualización de inventarios en tiempo real | | |
| | Visibilidad completa para prevenir la TI en la sombra | | |
| | Clasificación y categorización de activos | | |

| | | | |
|---|---|---|---|
| Gestión de existencias | Seguimiento y análisis del uso de aplicaciones | | |
| | Supervisión de la utilización de licencias | | |
| | Gestión de la configuración | | |
| | Seguimiento del control de versiones | | |

### 4.2 Control e informes continuos

***Consejo: Crítico para mantener la conciencia de seguridad en tiempo real a través de la supervisión activa, la detección inmediata de amenazas y las capacidades de informes integrales que impulsan conocimientos procesables.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Control en tiempo real | Detección de problemas de seguridad y alertas | | |
| | Exploración continua del entorno | | |
| | Control del rendimiento | | |
| | Seguimiento de los cambios de configuración | | |
| Capacidad de elaboración de informes | Informes de detección de anomalías | | |
| | Generación de informes personalizables | | |
| | Cuadros de mando específicos para las partes interesadas | | |
| | Análisis de tendencias y métricas | | |

### 4.3 Supervisión de la actividad de los usuarios

***Consejo: La supervisión del comportamiento de los usuarios constituye la piedra angular de la inteligencia de seguridad, ya que permite detectar rápidamente actividades sospechosas y posibles violaciones de la seguridad mediante el análisis de patrones.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Detección de comportamientos | Control de actividades sospechosas en tiempo real | | |
| | Análisis de los patrones de acceso de los usuarios | | |
| | Establecimiento de una línea de base conductual | | |
| | Detección de anomalías | | |
| Respuesta de seguridad | Identificación rápida de infracciones | | |
| | Generación automática de alertas | | |
| | Flujo de trabajo de respuesta a incidentes | | |
| | Registros de auditoría de la actividad de los usuarios | | |

### 4.4 Controles de Prevención de Pérdida de Datos (DLP)

***Consejo: Los controles de DLP deben proporcionar una protección completa contra las fugas de datos tanto accidentales como malintencionadas, manteniendo al mismo tiempo la productividad de la empresa mediante la aplicación inteligente de políticas.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Aplicación de la política | Creación y gestión de políticas de DLP | | |
| | Identificación de datos sensibles | | |
| | Automatización de la aplicación de políticas | | |
| | Creación de reglas personalizadas | | |
| Protección de datos | Prevención de fugas accidentales | | |

| | | | |
|---|---|---|---|
| | Prevención de filtraciones malintencionadas | | |
| | Clasificación de los datos | | |
| | Inspección de contenidos | | |

### 4.5 Control del cumplimiento

***Consejo: La supervisión automatizada del cumplimiento debe realizar un seguimiento continuo del cumplimiento de los requisitos normativos y, al mismo tiempo, proporcionar una visibilidad clara del estado de cumplimiento y de las necesidades de corrección.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Seguimiento del cumplimiento | Control continuo de la postura | | |
| | Cumplimiento de la normativa del sector | | |
| | Cuadro de mandos de cumplimiento | | |
| | Análisis de carencias | | |
| Gestión normativa | Controles específicos del marco | | |
| | Informes de cumplimiento automatizados | | |
| | Aplicación de la política | | |
| | Mantenimiento de registros de auditoría | | |

### 4.6 Gestión de contraseñas y accesos

***Consejo: Las políticas de contraseñas y la gestión de accesos deben equilibrar la seguridad con la facilidad de uso, garantizando una sólida protección contra accesos no autorizados y manteniendo la productividad de los usuarios.***

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

| | | | |
|---|---|---|---|
| Protección por contraseña | Detección de contraseñas débiles | | |
| | Análisis de la seguridad de las contraseñas | | |
| | Aplicación de la actualización de contraseñas | | |
| | Cumplimiento de la política de contraseñas | | |
| Aplicación de la política | Aplicación de una política estricta de contraseñas | | |
| | Gestión de la caducidad de contraseñas | | |
| | Aplicación del historial de contraseñas | | |
| | Reglas de complejidad de las contraseñas | | |

### 4.7 Evaluación de riesgos y medidas correctoras

***Consejo: Los sistemas de evaluación de riesgos deben proporcionar información procesable a través de una puntuación de gravedad precisa y rutas de corrección claras, permitiendo a las organizaciones centrarse primero en los problemas de seguridad más críticos.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Evaluación de riesgos | Análisis de la gravedad de los riesgos de seguridad | | |
| | Calificación de riesgos en tiempo real | | |
| | Evaluación de la vulnerabilidad | | |
| | Priorización de amenazas | | |
| Remediación | Orientación automatizada para la corrección | | |
| | Priorización de acciones | | |
| | Gestión del flujo de trabajo de corrección | | |

| | | | |
|---|---|---|---|
| | Verificación de la reparación | | |

### 4.8 Capacidades de integración

***Consejo: las capacidades de integración deben permitir una conexión perfecta con la infraestructura de seguridad existente, al tiempo que deben ser lo suficientemente flexibles como para adaptarse a las nuevas aplicaciones y a la evolución de las necesidades de seguridad.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Integración de SaaS | Integración perfecta de aplicaciones | | |
| | Conectividad basada en API | | |
| | Integración personalizada | | |
| | Sincronización de datos en tiempo real | | |
| Adaptabilidad | Soporte para nuevas aplicaciones | | |
| | Escalabilidad de la integración | | |
| | Compatibilidad multiplataforma | | |
| | Supervisión de la integración | | |

### 4.9 Control de acceso de terceros

***Consejo: La gestión del acceso de terceros requiere un control granular y una supervisión continua para minimizar los riesgos de seguridad al tiempo que se mantienen las relaciones empresariales necesarias.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Visibilidad de acceso | Supervisión de aplicaciones por terceros | | |
| | Seguimiento de los permisos de acceso | | |
| | Análisis de uso | | |

| | | | |
|---|---|---|---|
| | Evaluación de riesgos | | |
| Gestión de accesos | Gestión de permisos | | |
| | Funciones de revocación de acceso | | |
| | Automatización de la revisión de accesos | | |
| | Gestión del ciclo de vida del acceso de proveedores | | |

### 4.10 Inspecciones de seguridad

***Consejo: Las inspecciones de seguridad exhaustivas deben abarcar todos los aspectos de la postura de seguridad, garantizando al mismo tiempo el cumplimiento de la normativa y las normas del sector pertinentes.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Control de acceso | Inspección de la política de acceso | | |
| | Auditoría de permisos | | |
| | Control de acceso basado en funciones | | |
| | Verificación de autenticación | | |
| Protección de datos | Inspección DLP | | |
| | Análisis antivirus | | |
| | Verificación del cifrado | | |
| | Cumplimiento de la normativa sobre tratamiento de datos | | |

### 4.11 Corrección automatizada

***Consejo: La corrección automatizada debe minimizar la intervención manual y, al mismo tiempo, garantizar la precisión y mantener pistas de auditoría claras de todas las acciones automatizadas realizadas.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Automatización | Corrección de errores de configuración | | |
| | Aplicación de la política | | |
| | Implantación de parches de seguridad | | |
| | Normalización de la configuración | | |
| Gestión de alertas | Generación de alertas claras | | |
| | Reducción de falsos positivos | | |
| | Priorización de alertas | | |
| | Seguimiento de la reparación | | |

### 4.12 Escalabilidad

***Consejo: Las funciones de escalabilidad deben garantizar un rendimiento y una seguridad constantes a medida que crece la organización, gestionando el aumento de la carga sin comprometer la eficacia.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Apoyo al crecimiento | Ampliación de la base de aplicaciones | | |
| | Gestión del volumen de usuarios | | |
| | Mantenimiento de las prestaciones | | |
| | Optimización de recursos | | |
| Adaptación al medio ambiente | Escalado del entorno de nube | | |
| | Flexibilidad de las infraestructuras | | |
| | Equilibrio de la carga | | |
| | Planificación de capacidades | | |

### 4.13 Seguridad de la API

***Consejo: La seguridad de la API debe garantizar la transmisión segura de los datos y, al mismo tiempo, mantener una supervisión y un control exhaustivos de todas las interacciones de la API.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Control de acceso | Supervisión del acceso a la API | | |
| | Aplicación de la autenticación | | |
| | Gestión de autorizaciones | | |
| | Limitación de velocidad | | |
| Seguridad de los datos | Aplicación de la política de intercambio de datos | | |
| | Codificación del tráfico | | |
| | Validación de datos | | |
| | Pruebas de seguridad | | |

### 4.14 Aprendizaje automático e integración de la IA

***Consejo: Las capacidades de IA/ML deben mejorar la detección y prevención de amenazas, al tiempo que proporcionan información procesable a través de análisis avanzados y reconocimiento de patrones.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Detección de amenazas | Detección por ML | | |
| | Reconocimiento de patrones | | |
| | Análisis del comportamiento | | |
| | Análisis predictivo | | |
| Prevención | Identificación de nuevas amenazas | | |
| | Respuesta automática | | |

| | | | |
|---|---|---|---|
| | Predicción del riesgo | | |
| | Aprendizaje continuo | | |

### 4.15 Automatización del cumplimiento

***Consejo: La automatización del cumplimiento debe agilizar la adhesión a múltiples marcos normativos, manteniendo al mismo tiempo una documentación precisa y pruebas del cumplimiento.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Informes | Informes de cumplimiento automatizados | | |
| | Plantillas específicas | | |
| | Generación de informes personalizados | | |
| | Recogida de pruebas | | |
| Gestión estándar | Ajustes de conformidad preconfigurados | | |
| | Subsanación de deficiencias | | |
| | Cartografía de control | | |
| | Control del cumplimiento | | |

### 4.16 Evaluación de riesgos basada en IA

***Consejo: La evaluación de riesgos impulsada por IA debe proporcionar una visión profunda de la postura de seguridad, al tiempo que mantiene la precisión y proporciona una guía clara de remediación.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Análisis de riesgos | Evaluación de riesgos de aplicaciones de terceros | | |
| | Evaluación de las extensiones del navegador | | |
| | Automatización de la calificación de riesgos | | |

| | | | |
|---|---|---|---|
| | Priorización de amenazas | | |
| Informes de evaluación | Informes de riesgo automatizados | | |
| | Análisis del cumplimiento de la seguridad | | |
| | Tendencia del riesgo | | |
| | Recomendaciones de reparación | | |

### 4.17 Gestión de la postura de seguridad de la IA

***Consejo: AI-SPM debe proporcionar una visibilidad y protección completas de los activos de IA al tiempo que mantiene un inventario detallado y controles de seguridad.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Visibilidad de la IA | Seguimiento del despliegue de modelos | | |
| | Seguimiento del proyecto | | |
| | Detección de riesgos | | |
| | Control de acceso | | |
| Gestión de activos | Mantenimiento del inventario de IA | | |
| | Gestión de listas de materiales | | |
| | Seguimiento de la configuración | | |
| | Evaluación de la seguridad | | |

### 4.18 Seguridad del modelo de IA

***Consejo: La seguridad de los modelos de IA debe garantizar una protección completa de las configuraciones y los datos de los modelos, al tiempo que se mantienen estrictos controles de acceso y supervisión.***

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

| | | | |
|---|---|---|---|
| Seguridad de la configuración | Implantación de la seguridad de la red | | |
| | Medidas de protección de datos | | |
| | Gestión del control de acceso | | |
| | Auditoría de configuración de modelos | | |
| Supervisión | Supervisión de las claves de acceso | | |
| | Detección de datos sensibles | | |
| | Seguimiento de la utilización | | |
| | Alertas de seguridad | | |

### 4.19 Gestión de aplicaciones GenAI

***Consejo: La gestión de aplicaciones GenAI debe proporcionar control y seguridad de nivel empresarial, manteniendo al mismo tiempo la flexibilidad para el uso legítimo del negocio.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Gestión de cuentas | Configuración de la cuenta de empresa | | |
| | Control de acceso de usuarios | | |
| | Gestión del grupo | | |
| | Aplicación de la política | | |
| Controles de seguridad | Gestión de la política de autenticación | | |
| | Aplicación de la AMF | | |
| | Seguimiento de la utilización | | |
| | Revisiones de acceso | | |

### 4.20 GPT personalizada y gestión de plugins

***Consejo: La gestión personalizada de GPT debe permitir la creación y despliegue seguros, manteniendo un control estricto sobre las integraciones de terceros y el acceso al mercado.***

| Requisito | Subrequisito | S/N | Notas |
|---|---|---|---|
| Gestión de GPT | Soporte para la creación de GPT personalizadas | | |
| | Gestión de plugins | | |
| | Control de versiones | | |
| | Validación de seguridad | | |
| Control de acceso | Gestión de acceso al mercado | | |
| | Autorización de plugins | | |
| | Restricciones de uso | | |
| | Aplicación de la política | | |

## 5. 5. Consideraciones adicionales

### 5.1 Integración con las infraestructuras existentes

- Descripción de los métodos de integración
- Plataformas y sistemas compatibles
- Documentación API
- Calendario de integración

### 5.2 Experiencia del usuario y facilidad de uso

- Diseño de interfaces
- Requisitos de formación
- Controles administrativos
- Optimización del flujo de trabajo del usuario

### 5.3 Escalabilidad y rendimiento

- Alojamiento de crecimiento
- Métricas de rendimiento
- Recursos necesarios
- Planificación de capacidades

### 5.4 Asistencia y mantenimiento

- Opciones de asistencia
- Tiempos de respuesta
- Frecuencia de actualización
- Ventanas de mantenimiento

### 5.5 Modelo de fijación de precios

- Estructura de la licencia
- Costes de aplicación
- Cuotas de mantenimiento
- Costes adicionales del servicio

### 5.6 Conformidad y certificaciones

- Certificaciones del sector
- Marcos de cumplimiento
- Apoyo a las auditorías
- Requisitos reglamentarios

### 5.7 Informes y análisis

- Informes estándar
- Informes personalizados
- Capacidades analíticas
- Personalización del cuadro de mandos

### 5.8 Protección de datos

- Procedimientos de tratamiento de datos
- Controles de privacidad
- Residencia de datos
- Métodos de cifrado

## 6. 6. Criterios de evaluación

Las propuestas se evaluarán en función de

1. Solución completa
2. Capacidad de integración
3. Compatibilidad del sistema
4. Facilidad de uso
5. Requisitos de formación
6. Métricas de escalabilidad
7. Parámetros de rendimiento
8. Ofertas de apoyo
9. Coste total de propiedad
10. Experiencia del proveedor
11. Reputación del mercado

## 7. Instrucciones de presentación

Los vendedores deben proporcionar:

1. Descripción detallada de la solución
2. Especificaciones técnicas
3. Plan de aplicación
4. Enfoque de la formación
5. Detalles de asistencia

6. Estructura de precios
7. Perfil de la empresa
8. Referencias de clientes
9. Documentación de muestra
10. Calendario del proyecto

## 8. Cronología

- Fecha de publicación de la RFP:
- Plazo de preguntas:
- Fecha límite para la presentación de propuestas:
- Presentaciones de proveedores:
- Selección final:
- Inicio del proyecto:

## 9. 9. Información de contacto

Si tiene preguntas sobre esta solicitud de propuestas, póngase en contacto con

Fin del documento de solicitud de propuestas