M S S P

Managed Security Services Providers

Proveedores de Servicios de Seguridad Gestionados

1

¿Qué es un MSSP?

Un Proveedor de Servicios de Seguridad Gestionada (MSSP, por sus siglas en inglés) es una empresa que ofrece servicios de seguridad para proteger la infraestructura de TI de sus clientes.

Los MSSPs ayudan a las organizaciones a gestionar y monitorizar su seguridad de forma continua, utilizando una combinación de tecnologías avanzadas y expertos en seguridad.

Los servicios de los MSSPs son especialmente valiosos para empresas que no tienen los recursos internos para manejar todos los aspectos de la ciberseguridad por sí mismas.

2

Razones a Favor de Contratar un MSSP

3

Acceso a Experiencia Especializada: Los MSSPs cuentan con equipos de profesionales altamente cualificados y con experiencia en diferentes áreas de la ciberseguridad. Esto es especialmente útil para organizaciones que no tienen los recursos internos para contratar y retener talento especializado.

Monitoreo Continuo y Respuesta Rápida: Los MSSPs ofrecen monitoreo 24/7, lo que garantiza que cualquier amenaza potencial se detecte y se responda rápidamente, incluso fuera del horario laboral normal. Proporcionan servicios de respuesta a incidentes que pueden mitigar los daños en caso de un ataque.

Eficiencia Operativa y Costos Razonables: Contratar un MSSP puede ser más económico que construir y mantener un equipo interno de ciberseguridad, especialmente para pequeñas y medianas empresas. Permite a la empresa enfocarse en su negocio principal mientras delega la seguridad a expertos.

Tecnología Avanzada: Los MSSPs utilizan herramientas y tecnologías avanzadas que pueden ser costosas de adquirir y mantener para una organización individual. Estas herramientas incluyen sistemas de gestión de información y eventos de seguridad (SIEM), detección de intrusos, análisis de amenazas, entre otros.

Cumplimiento Normativo: Los MSSPs ayudan a las organizaciones a cumplir con regulaciones y estándares de seguridad, proporcionando experiencia en auditorías, reportes y mantenimiento de cumplimiento.

Escalabilidad y Flexibilidad: Los MSSPs pueden escalar sus servicios según las necesidades de la organización, proporcionando flexibilidad para adaptarse a cambios en el tamaño o la complejidad de la empresa.

4

Inconvenientes y Riesgos de Contratar un MSSP

5

Pérdida de Control: Al delegar la seguridad a un proveedor externo, la organización puede sentir que pierde control sobre ciertos aspectos de su infraestructura de seguridad. Es crucial establecer acuerdos de nivel de servicio (SLAs) claros para asegurar que el MSSP cumpla con las expectativas de rendimiento y seguridad.

Dependencia del Proveedor (¿?): La organización puede volverse dependiente del proveedor para la gestión de su seguridad, lo que puede ser problemático si la relación contractual termina o si el proveedor no cumple con sus expectativas.

Integración y Compatibilidad: Puede haber desafíos en la integración de las soluciones del MSSP con los sistemas y procesos internos de la organización. Es importante asegurarse de que el MSSP pueda trabajar bien con la infraestructura tecnológica existente.

Riesgos de Confidencialidad y Privacidad: Transmitir datos sensibles a un proveedor externo puede aumentar los riesgos de privacidad y confidencialidad. Es fundamental seleccionar un MSSP con fuertes políticas de protección de datos y un historial comprobado de seguridad.

Calidad del Servicio y Visibilidad: La calidad de los servicios puede variar según el proveedor, y es importante evaluar la reputación y experiencia del MSSP antes de contratarlo. La organización debe asegurarse de que el MSSP proporcione visibilidad y transparencia adecuadas en sus operaciones y reportes.

6

Servicios Típicos de un MSSP I

7

Monitoreo y Gestión de Seguridad 24/7

Vigilancia continua de redes, sistemas y aplicaciones para detectar y responder a amenazas en tiempo real.

Gestión de Incidentes y Respuesta a Incidentes

Provisión de servicios para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad.

Gestión de Vulnerabilidades

Escaneo regular de vulnerabilidades y evaluación de la seguridad para identificar y remediar debilidades en los sistemas.

Gestión de Dispositivos de Seguridad

Configuración, monitoreo y mantenimiento de dispositivos de seguridad como firewalls, sistemas de prevención de intrusiones (IPS), y sistemas de detección de intrusiones (IDS).

8

Servicios de Inteligencia de Amenazas

Provisión de información actualizada sobre amenazas emergentes y tácticas de ataque para ayudar a las organizaciones a anticipar y mitigar riesgos.

Análisis y Gestión de Logs

Recolección, análisis y almacenamiento de logs de seguridad para detectar actividades sospechosas y cumplir con regulaciones.

Evaluaciones de Seguridad y Pruebas de Penetración

Realización de pruebas para identificar vulnerabilidades y evaluar la eficacia de las medidas de seguridad existentes.

Cumplimiento Normativo

Ayuda para cumplir con regulaciones y estándares de seguridad, como GDPR, PCI-DSS, HIPAA, entre otros.

Consultoría de Seguridad

Servicios de asesoramiento para diseñar e implementar estrategias de seguridad y políticas efectivas.

9

Criterios para Evaluar un Potencial MSSP

10

Experiencia y Reputación

Investigar el historial y la reputación del MSSP en la industria.

Revisar testimonios, estudios de caso y referencias de clientes actuales y anteriores.

Certificaciones y Cumplimiento

Verificar que el MSSP tenga certificaciones relevantes como ISO 27001, PCI DSS, entre otras.

Verificar que cumplan con las normativas y estándares que son importantes para su industria.

Alcance de los Servicios

Evaluar si los servicios ofrecidos por el MSSP cubren todas sus necesidades de seguridad actuales y futuras.

Considerar la flexibilidad y la capacidad del proveedor para escalar los servicios según sea necesario.

Tecnología y Herramientas

Revisar las tecnologías y herramientas que utiliza el MSSP para la protección y monitorización.

Verificar que están utilizando tecnologías avanzadas y que se integren bien con sus sistemas existentes.

11

Capacidad de Respuesta y Soporte

Evaluar la capacidad del MSSP para responder rápidamente a incidentes de seguridad.

Revisar los acuerdos de nivel de servicio (SLAs) y la disponibilidad del soporte técnico.

Costos y Modelos de Precios

Considerar los costos de los servicios en relación con su presupuesto.

Evaluar los modelos de precios (por ejemplo, precios fijos, basados en el uso) para ver cuál se adapta mejor a sus necesidades.

Transparencia y Comunicación

Evaluar la transparencia del MSSP en la presentación de informes y comunicación.

Verificar que proporcionen informes regulares y detallados sobre la seguridad y el rendimiento.

Adaptabilidad y Personalización

Verificar que el MSSP pueda adaptar sus servicios a sus necesidades específicas y personalizar las soluciones de seguridad.

Visión y Estrategia de Seguridad

Evaluar la visión y estrategia a largo plazo del MSSP en ciberseguridad.

Asegurarse de que estén alineados con sus objetivos y prioridades de seguridad.

12

Inicialmente, el costo más bajo fue el principal impulsor para pasar a un proveedor de servicios administrados, pero el costo solo ocupa el cuarto lugar en los criterios de decisión actuales.

Mejorar la calidad de la protección. Algunas organizaciones simplemente no tienen la experiencia en seguridad deseada en ciertas áreas o no pueden pagarla, lo que genera grandes brechas en la cartera de seguridad. En lugar de invertir internamente, un MSSP puede ayudar a llenar los vacíos y reducir la carga de trabajo de los recursos existentes.

Obtener soporte 24x7. El panorama de amenazas se ha vuelto demasiado complejo y sofisticado para confiar en un modelo de soporte de seguridad de 9 a 17.

Obtener mejores conjuntos de habilidades y competencias. Es importante comprender el hecho de que el personal no puede ser competente en todos los aspectos de la seguridad. Los analistas de seguridad de las compañías de seguridad administradas tienen más profundidad, amplitud y experiencia porque tratan con una amplia variedad de clientes y entornos.

Reducir costos. Las continuas presiones económicas han obligado a muchas organizaciones de seguridad a reducirse significativamente, ya sea en forma de recortes presupuestarios, reducción de personal o, en algunos casos, ambos. Enfrentados con menos recursos, muchas organizaciones de seguridad se han visto obligadas a emplear MSS para cumplir con sus obligaciones.

13

Es ideal que se pueda **probar** el potencial del servicio con una pequeña función o tarea que no sea crítica para el negocio. Si esa experiencia resulta positiva, la empresa puede considerar la posibilidad de ampliar la gama de servicios a tercerizar.

El proceso de **implementación** tiene varios componentes, cuyos costos deben ser reconocidos e incluidos en el análisis a realizar.

La **fase de transición es q**uizás la fase menos comprendida y subestimada del proceso de subcontratación.

14

Gobierno de la Seguridad y los MSSP

La gobernanza de la seguridad de la información en la capa de estrategia no puede subcontratarse porque la responsabilidad final siempre recae en la propia organización.

La alta gerencia de la Organización es en última instancia responsable de la Seguridad de la Información de la Organización y la protección de sus activos, ya que entienden la visión de la empresa y los objetivos comerciales.

En última instancia, todas las consecuencias de no implementar adecuadamente la Seguridad de la Información son asumidas por la organización y no por el proveedor.

15

Ser específico en sus requisitos y consecuencias de incumplimiento de contrato

Establecer "accountability" al compartir la responsabilidad.

Definir problemas y procesos de resolución de problemas.

Comprometer con la protección de datos y los requisitos de cumplimiento.

Especificar requisitos de personal y competencias.

Asegurar un monitoreo y cumplimiento consistentes a través de la comunicación y la coordinación.

16