

MIGESA Azure Risk & Compliance Assessment



Soluciones
Microsoft



Los datos son uno de los activos más valiosos que una empresa tiene y es de suma importancia considerar mantenerla bajo un sistema de seguridad, lo que resulta cada vez más complejo.



Desafíos

El ciberespacio es el nuevo campo de batalla y que hay que asumir los retos por venir:

Cada vez que los clientes migran servidores, aplicaciones a la nube, o adoptan una nueva infraestructura, representa un desafío de seguridad

El home office representa un reto debido a que los empleados se encuentran fuera del ambiente de control de las empresas.

La falta de estrategia y controles de seguridad cibernética.

Evitar interrupciones de servicio costosas.



Solución ideal

Adoptar estrategias efectivas y seguras para su entorno en la nube:

Lograr que las políticas de seguridad sean plenamente efectivas.

Visión panorámica de puntos ciegos de la infraestructura

Nos ayuda a un aseguramiento y valoración continua del nivel de riesgo

Garantiza a los clientes un conocimiento profundo y detallado de su ecosistema en la nube, así como un control, sobre la seguridad y la integridad de los datos.



Resultados deseados

En la ciberseguridad la conciencia y la participación de los colaboradores es crucial:

- Incrementa la disponibilidad de la operación y servicio de tu empresa.
- Identifica y reduce riesgos que puedan afectar a tu negocio.

Nos ayuda a conocer el nivel de exposición de riesgo **actual** ante las amenazas internas y externas.

Ayudar a la toma de decisiones proactivas y estratégicas en el entorno de la ciberseguridad.



Existen dos tipos de empresa, las que han sido hackeadas y las que no saben que han sido hackeadas. Por ello la evaluación a fondo de su infraestructura de nube es crucial para detectar y mitigar amenazas en este servicio combinamos nuestra experiencia con las herramientas de seguridad de Microsoft.

Los ciberataques, el fraude y robo de datos son tan probables como los desastres naturales, se encuentran en el top 5 de los riesgos globales con mayor probabilidad y de alto impacto, según el reporte The Global Risk Landscape 2019 del Foro Económico Mundial. Por tal motivo, las organizaciones deben estar conscientes del significado de estos datos duros y tomar las acciones prioritarias que les permita desarrollar una estrategia de seguridad holística bien alineada a los objetivos de negocio.

Descubrimiento

- Análisis del entorno de seguridad (entrevistas y cuestionarios)
- Análisis de plataformas adquiridas
- Descubrimiento / identificación de Stakeholders y definición de: Prioridades, Alcances, Expectativas y Entregables

Aanálisis

- Ejecución y Análisis de Microsoft Security Center.
- Evaluación de Regulación y Cumplimiento acorde a las mejores practicas recomendadas por Microsoft.
- Identificación de brechas riesgos y vulnerabilidades de seguridad.

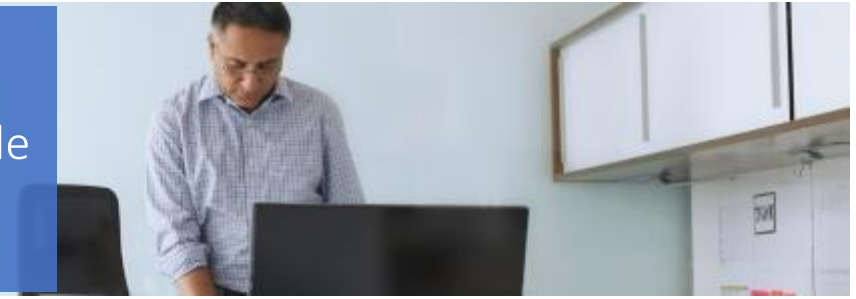
Reportes

- Un anteproyectos con las arquitecturas requeridas de protección y mitigación de riesgos que incluye:
- Recomendaciones claras y detalladas acerca de brechas, riesgos y vulnerabilidades de seguridad encontradas.
 - Presentación de resultados de Azure Security Center.

Investigar otra opcion

MIGESA Azure Risk & Compliance Assessment

Los servicios de nube y el consumo de internet, son una gran necesidad para cualquier empresa. Pero esto implica que la continuidad del negocio, datos de clientes o de empleados estén expuestos a nuevos riesgos. Entonces, ¿Qué hacer?



Azure Risk & Compliance Assessment es un conjunto de servicios que permiten alinear la estrategia de seguridad de las compañías mediante la generación de un assessment de seguridad que proporciona un road map de implementación, uso, consumo y adopción de los servicios que se usan actualmente en Microsoft Azure, casos de uso por industria, mejores prácticas y recomendaciones con base en estándares internacionales tales como ISO 27000, ISO 31000, NIST y CSF.

Alineación de la Solución

Confidencialidad

Es la propiedad Impedir la divulgación de información a personas o sistemas no autorizados

- Identificar activos de negocio.
- Controles de seguridad



Integridad

Mantener nuestros datos libres de modificaciones no autorizadas

- Hardening de infraestructura y aplicaciones
- Cifrado de datos y comunicación garantizada, que la información no será modificada por personas no autorizadas



Disponibilidad

Contar con la información a nuestra disposición con los accesos correctos

- Acceso a personas, procesos o aplicaciones
- Permite que la información este disponible cuando sea necesario

