Cloud Security
Compliance

pyxis

Pyxis Cloud Security Compliance

Hoy en día el entorno corporativo requiere en muchas ocasiones cumplir con distintos estándares para dar cumplimiento normativo sobre el negocio que desarrollan, por ejemplo: PCI-DSS, HIPAA, SOX. Estos requerimientos están enfocados en la protección de los activos de información, por lo que es necesario sumar un análisis especifico adicional a las buenas prácticas de seguridad en Cloud.

El servicio Compliance (CSC) incluye los servicios de Assessment (CSA) e implementación (CSD) y los complementa desde el inicio considerando el cumplimiento del estándar que el cliente requiera.

CSC permite confirmar el cumplimiento de la norma o estándar de forma explícita a través de ejecución de pruebas sobre las soluciones a certificar.

- Cloud Security Approach
- Cloud Security Deployment

A continuación se describen las fases que componen el servicios de Compliance:

Alcance y Estándar
Lo primero que se debe establecer es el marco regulatorio exigido (estándar a cumplir) y el alcance que tendrá en la nueva infraestructura Cloud del cliente. El cumplimiento se aplica generalmente a los activos de información en relación al estándar que se sigue, por tanto en esta fase se debe acordar con el cliente el alcance de cumplimiento de las soluciones a desplegar en la nueva infraestructura.

Cumplimiento
La última fase de este servicio es la confirmación de cumplimiento del estándar de forma empírica, ya en la infraestructura implantada y con las soluciones operativas. Para esto se ejecutarán actividades de chequeo configuraciones, accesos y procedimientos importantes para los procesos de auditoría.

Microsoft Partner

Gold Cloud Platform
Gold Datacenter
Gold Cloud Productivity
Gold Small and Midmarket Cloud Solutions

Powered By:

Ver en:
Azure Marketplace

Más Información:
www.pyxis.com.uy/cloud-security