

Pyxis Cloud Security Approach

It is currently important and increasingly necessary to follow and implement the good practices of security in Information Technology, particularly for cloud environments, providers comply with various security standards that apply to their data centers, although they leave the responsibility to their clients to a greater or lesser extent on the final security configurations.

Also, it is a common practice that the cloud approach of many companies follow the guidelines of the business, without considering the security from the early stages of defining architecture and infrastructure. As a more immediate consequence, a very high percentage of the incidents of security happens due to poor service configurations or with their default values.

Cloud Security Approach proposes a mandatory look at the infrastructure and services deployed in the Cloud, as well as a vision with the premises of Security by Default and Zero Trust for new solutions. Through the CSA, opportunities for improvement related to the client's infrastructure are identified and weighed, recommending a design that complies with good practices and updated security standards.

The phases that make up the CSA are described below:

1.- Current Situation Assessment

A starting point to know the reality of the client, understand the needs and challenges that the client's infrastructure currently has, as well as the new requirements and improvement options that it hopes to obtain. In this way, we work together on definitions of the new Cloud solutions that best suit the business.

2.- Safe Infrastructure Design

Cloud infrastructure development brings with it a set of practices and ways of working that are not fully comparable or equivalent to on-premise scenarios. Therefore, it is necessary to understand how the current reality of the client adapts to a Cloud environment. New forms of access will be considered, identity management, and other aspects that make up the design of information security in the Cloud.

This is the main phase of the CSA, where the design that best suits the client's needs is defined, considering and prioritizing security according to the best practices and experiences in the area.

3.- Improvement Recommendations

After achieving a design according to the client, the recommendations for improvement will be presented, emphasizing the benefits that will be obtained with the new infrastructure, the considerations that must be taken into account, and other changes that the new configuration may imply.

4.- Accompaniment in the Implementation Strategy

We trust that this phase will generate the most important added value for the client, where the guidelines suggested in the previous phases will be followed, a new stable and reliable solution will be achieved with the security guarantees that have been agreed upon.

We join the client in these first steps, advising and clearing up any doubts that may arise during the implementation stage.

Microsoft
Partner

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



Cloud Security
Approach

Powered By: 

More Information:
www.pyxis.com.uy/cloud-security

View in:
[Azure Marketplace](#)