ADVANCED ACCESS INDETITY MANAGEMENT MODEL ON AWS (IAM)

\*Analysis and development of a proposed multilevel security model based on the advanced access identity management model

# 1st Freddy Leonel Pachacama

*dept. Computer´s Science Application of Operating Systems*

Sangolquí, Ecuador

flpachacama@espe.edu.ec

# 1st Kevin Quimuña

*dept. Computer´s Science Application of Operating Systems*

Sangolquí, Ecuador

kfquimuna@espe.edu.ec

***Abstract*—The purpose of this project is to implement a multilevel security model based on the organizational structure of the company Cayambito dedicated to has to offer traditional products of the sector. This through Aws as advanced access identity management tool, it is intended to also make known what it consists of and how a directory server. Within this framework it will be seen how to create a directory structure, database and its setting. The practical part will consist of the application of the theoretical part in an example of operation using two computers for this purpose in order to see the process of authentication. At the end of the project, a vision of what can be applied (IAM) will be obtained, as well as the recommendations necessary for its implementation.**

***Index Terms*—IAM, Security Multilevel, Method, Organization, hierarchy.**

1. GOALS
2. *General*

Analyze and develop a proposal for an advanced identity access management model (IAM)

1. *Specific*

Select a business model organization based on from which a hierarchy of levels of access to the information of the institution

Preparate an access and permission matrix according to the established hierarchy.

1. THEORETICAL FRAMEWORK

*A. Advanced access identity management model*

Also known as MLS (Multiple Level Security), is a type of security policy that classifies users into different security levels, allowing access simultaneous to different users with different permissions and making sure that each user accesses those resources that you are authorized to and in the manner that you are authorized to, for therefore it is a technology that allows to protect secrets and thus prevent any user from accessing certain information whose access you are not allowed. Security technology multilevel classifies the data using the information security levels: (Highest) Top secret, (High) Secret, (Lower) Confidential, (Lower) Unclassified. One is for refer to a system that is adequate to protect itself of subversion and has robust mechanisms for separating of information, that is, reliable. The other refers to a computer application that will require it to be strong enough to protect itself from subversion and which means adequate mechanisms to separate domains of information.

1. *IAM*

AWS identity and access management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage the permissions that control which AWS resources users can access.

1. MATERIALS
   * Laptops
   * Windows 11 Operating System
   * Internet Access
   * AWS account
2. Instructions
3. *Business Model*

* Select a business model or organization.

Cayambito is an Ecuadorian company dedicated to the production and distribution of traditional sweets with high quality standards at an affordable price, allowing wholesale and retail purchases.



Fig. 1. Cayambito Logo

* Establish a hierarchy of levels of access to the information of the institution.

The company hierarchy is as follows:

1. *Company Matrix*

* Prepare an access and permissions matrix according to the established hierarchy.

After analyzing the hierarcgy, the matrix of according to the levels that belong.

1. *Basic implementation to demonstrate the model according to the levels in AWS.*

* *Steps:*

1. We create an AWS account.
2. We create imagine to EC2 and S3
3. We are going to create new users, and we go to the IAM part.
4. We enter the username and select the type of access, finally we give a password.
5. On the next page we add the permissions, we can associate it to a group or give permissions to only one user.
6. We can add tags where they are labeled to each infrastructure of our company.
7. At the end we will have the review screen where we can see all the configurations that we have given to our user.
8. Once our user has been created, we can verify that it was created correctly simply by entering AWS again with the newly created account.

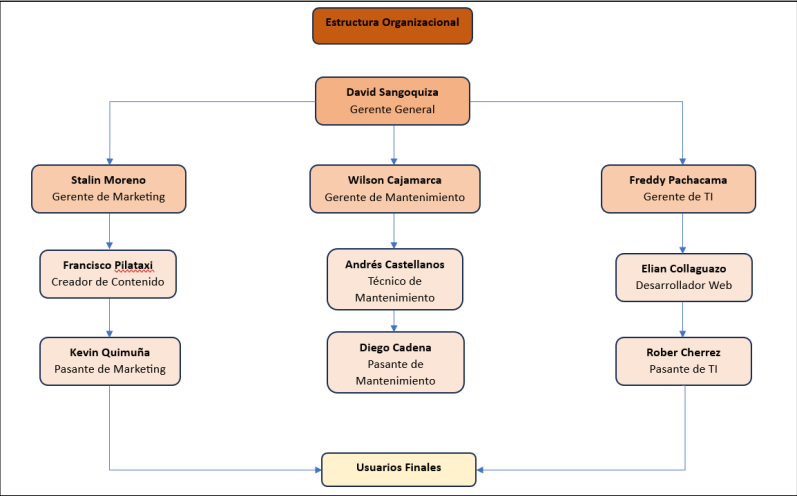
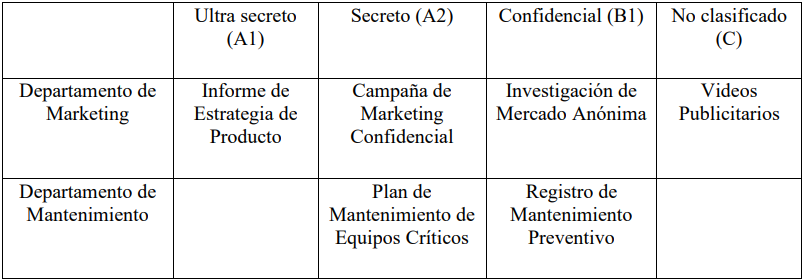


Fig. 2. Cayambito Hierarchy



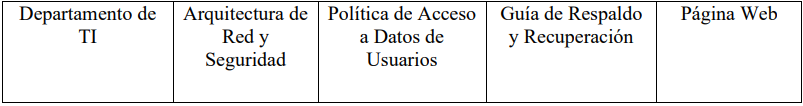


Fig. 3. Cayambito Matrix

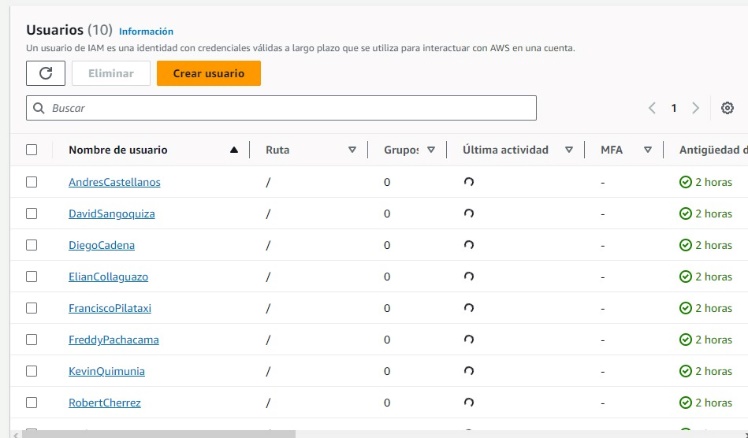
**

Fig. 4. Step 1

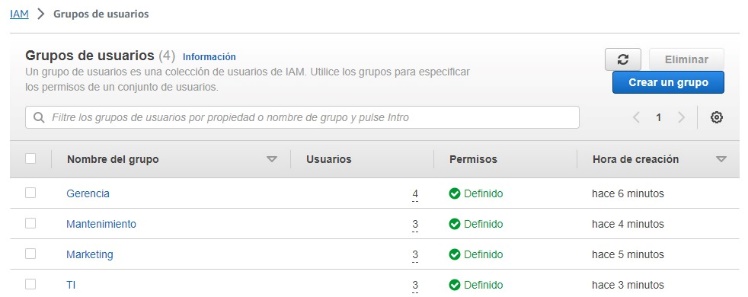
**

Fig. 5. Step 2

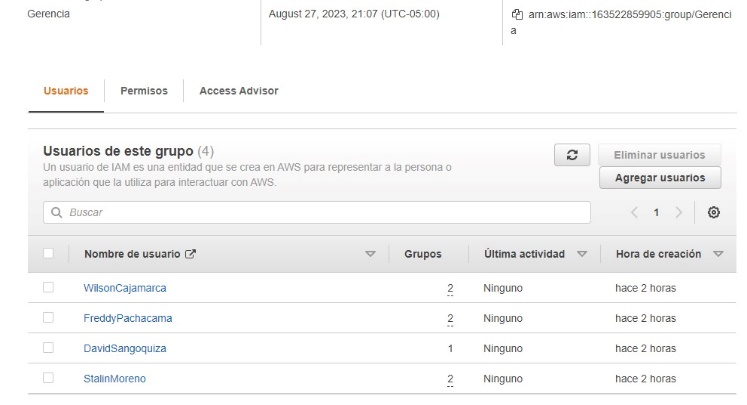
**

Fig. 6. Step 3

**

Fig. 7. Step 4

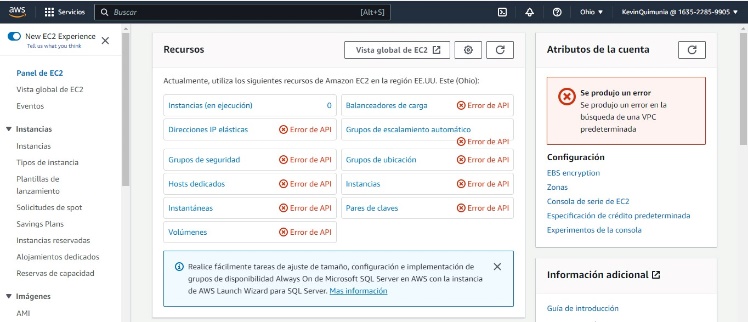
**

Fig. 8. Step 5

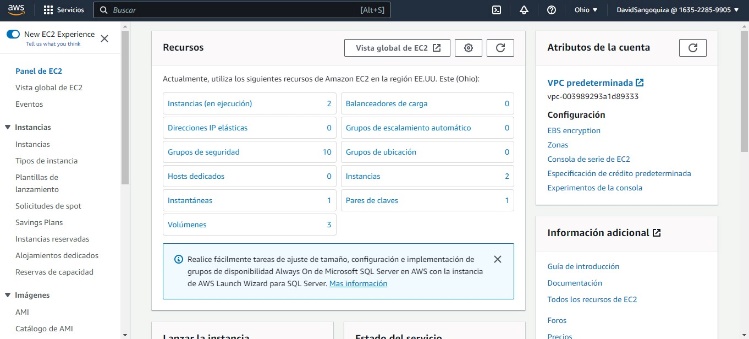
**

Fig. 9. Step 6

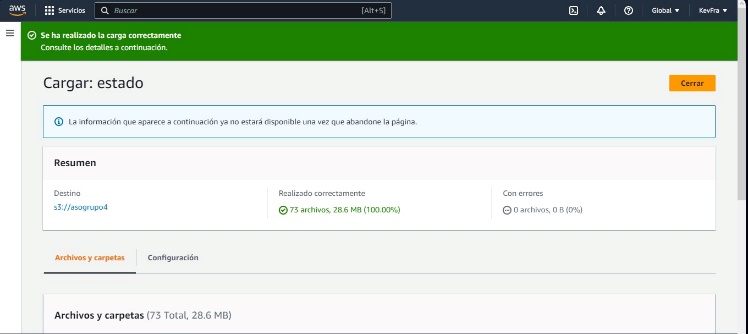
**

Fig. 10. Step 7

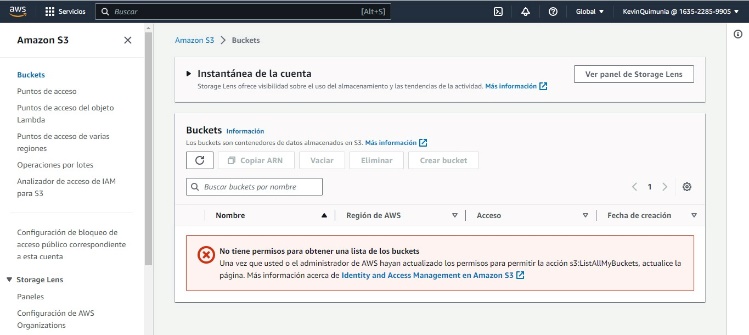
**

Fig. 11. Step 8

CONCLUSIONS

* It can be concluded that when carrying out this project we have knowledge of the most important theoretical concepts related to the advanced access methodology in AWS.
* After the installation tests, configurations and user creations, it is possible to understand and know how important, useful and practical it is to have a directory of users, in the case given of a company, or as of any other type of information.
* In AWS we find several preconfigured access lists, which can be used to practice giving access to users or groups of users.

RECOMMENDATIONS

* Always keep in mind how far the free limit in AWS goes in order to avoid unnecessary expenses.
* In case it is difficult to carry out the practice, there are several tutorials on digital platforms with very good explanations.
* For the creation of users, it is advisable to take into account what permissions you want to give and for whim that user will be directed.

REFERENCES

1. J. Lopez, “Seguridad multinivel´´, April 2008
2. G. Tugurium, “Bell-LaPadula model´´, December 2005
3. I. S. Jacobs “phpLDAPadmin”, September 2007