# opción

Revista de Antropología, Ciencias de la Comunicación y de la Información, Filosofía, Lingüística y Semiótica, Problemas del Desarrollo, la Ciencia y la Tecnología

Año 35, 2019, Especial N° 20
Revista de Ciencias Humanas y Sociales
ISSN 1012-1587/ ISSNe: 2477-9385
Depósito Legal pp 198402ZU45

Universidad del Zulia
Facultad Experimental de Ciencias
Departamento de Ciencias Humanas
Maracaibo - Venezuela

Opcion, Año 35, Nº Especial 20 (2019):*2899-2921*
ISSN 1012-1587/ISSNe: 2477-9385

# Green Cloud Computing Ideas with Security Threats and Solutions

**Robbi Rahim[1*], Fitri Masitoh[2], Alexei B. Kuzmichev[3], E. Laxmi Lydia[4], K. Shankar[5]**

**[1]Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia; usurobbi85@zoho.com**
**[2]Politeknik Penerbangan Palembang, Indonesia.**
**[3]Togliatti State University, Russia**
**[4]Professor, Vignan's Institute of Information Technology(A), Department of Computer Science and Engineering, Visakhapatnam, Andhra Pradesh, India; elaxmi2002@yahoo.com**
**[5]Department of Computer Applications, Alagappa University, India; shankarcrypto@gmail.com**

**Abstract**

**Cloud Computing gives the capacity to utilize computing and capacity assets on a metered premise and lessen the interests in an associations processing foundation. Cloud computing has been on the ascent for a long time yet the threats to this innovation are currently more unambiguous than any time in recent memory. On the off chance that the business is to be legitimized by the concerned native it should initially defeat a genuine of potential threats, past just cyber-crime. Peoples are not very much aware about the security issues and the dangers worried about cloud computing. It is by all accounts a tremendous boundary to the selection of cloud administrations. The data in regards to how to oversee information security inside a cloud, information protection in the cloud, cloud security principles, the administrative and consistence ramifications of relocating to a cloud model, and so on ought to be surely known before receiving the cloud administration and arrangements. This paper introduces a comprehension of this intricate situation and explains every one of these issues by distinguishing and ordering the fundamental security concerns and arrangements**

in cloud computing and gives complete direction on the best way to explore the field of cloud computing to accomplish the most extreme profit for cloud ventures without bargaining data security.

Keywords— Cloud computing; data privacy; security; service model; solutions;

## Ideas de computación en la nube verde con amenazas y soluciones de seguridad

Resumen: Cloud Computing brinda la capacidad de utilizar la computación y los activos de capacidad en una premisa medida y disminuye los intereses en una base de procesamiento de asociaciones. La computación en la nube ha estado en ascenso durante mucho tiempo, pero las amenazas a esta innovación son actualmente más inequívocas que nunca en la memoria reciente. En el caso de que el negocio en cuestión sea legitimado por el nativo en cuestión, inicialmente debe vencer a una verdadera amenaza potencial, más allá del cibercrimen. Los pueblos no son muy conscientes de los problemas de seguridad y los peligros preocupados por la computación en la nube. Es, a todas luces, un límite tremendo para la selección de las administraciones en la nube. Los datos con respecto a cómo supervisar la seguridad de la información dentro de una nube, la protección de la información en la nube, los principios de seguridad de la nube, las ramificaciones administrativas y de consistencia de la reubicación a un modelo de nube, etc., deben conocerse seguramente antes de recibir la administración de la nube y preparativos. Este documento presenta una comprensión de esta compleja situación y explica cada uno de estos problemas al distinguir y ordenar las preocupaciones y arreglos fundamentales de seguridad en la computación en la nube y brinda una dirección completa sobre la mejor manera de explorar el campo de la computación en la nube para lograr el beneficio más extremo para emprendimientos en la nube sin negociación de seguridad de datos.

Palabras clave: computación en la nube; privacidad de datos; seguridad; modelo de servicio; soluciones;

## I. INTRODUCTION

Cloud computing is an IT model or figuring condition made out of IT segments (equipment, programming, systems administration, and administrations) just as the procedures around the sending of these components that together empower us to create and convey cloud administrations by means of the Internet or a private system. The generating and cancellation of virtual machines running on physical equipment and being constrained by hypervisors is a cost-proficient and adaptable figuring worldview.
This cloud model is made out of five basic qualities, three administration models, and four deployment models. The five basic attributes are as per the following:

- On-request self-administration
- Ubiquitous network access
- Resource pooling
- Location autonomy
- Rapid elasticity
- Measured service

The administration models are as per the following:

a)Cloud Software as a Service (SaaS)—Use supplier's applications over a system.
b)Cloud Platform as a Service (PaaS) —Deploy client made applications to a cloud.
c)Cloud Infrastructure as a Service (IaaS) —Rent handling, stockpiling, organize limit, and other basic registering assets.

The deployment models, which can be either inside or remotely actualized, are abridged in the NIST introduction as pursues:

1. Private cloud—Enterprise claimed or rented.
2. Community cloud—Shared foundation for explicit network.
3. Public cloud—Sold to general society, super scale foundation.
4. Hybrid cloud—Composition of at least two mists.

With every one of its advantages, cloud computing additionally carries with it worries about the security and protection of data surviving on the cloud because of its size, structure, and topographical scattering.

This paper presents security issues experienced in cloud computing, and has an exploration on numerous specialized answers for cloud security issues. The remainder of this paper is sorted out as pursues. Area II proposes the extent of cloud computing security, gives an outline on cloud security industry, and talks about and records the different security dangers of cloud computing both on the clients and administrators. Area III examines numerous security specialized answers for defeat the difficulties from cloud security and so on. At that point area IV, a finish of the cloud computing security dangers and arrangements.

## II. CLOUD COMPUTING SECURITY CHALLENGES

Cloud computing framework and situations are less difficult that even organizations can get to the best-of-breed business applications by basically taking advantage of the cloud. It is likewise conceivable to share and advance their foundation assets at exceptionally low expenses. Despite the fact that it portrays the straightforwardness of cloud computing innovation, it really questions the security of the cloud condition.

The greater part of the agents are not very much aware about the security issues and the dangers worried about cloud computing. It is by all accounts an enormous hindrance to the selection of cloud administrations. The data in regards to how to oversee information security inside a cloud, information protection in the cloud, cloud security benchmarks, the administrative and consistence ramifications of relocating to a cloud model, and so forth ought to be surely known before receiving the cloud administration and arrangements.

In spite of the fact that a vast greater part of organizations are intending to build the quantity of cloud applications utilized in their associations, 71 percent concede they are utilizing cloud applications that have not been authorized by their IT divisions, as per a study of 200 IT and business experts on the appropriation, use and security of cloud applications led by character the board supplier and security consultancy.

With access to these applications occurring from an assortment of areas including Smartphone's (80 percent), tablets (71 percent) and non-organization PCs (80 percent) and with a huge level of associations (73 percent)

expecting to concede transitory access to cloud applications, respondents referred to worries around character the board, administration and multi-faceted nature.

"With endeavors quickly going to cloud applications, the inalienable dangers in practices like utilizing unsanctioned applications or sharing passwords on sticky notes should be tended to, and rapidly."

The study demonstrated hazardous secret phrase the executives keeps on being a test, with 43 percent of respondents conceding that representatives oversee passwords in spreadsheets or on sticky notes and 34 percent offer passwords with their collaborators for applications like FedEx, Twitter, Staples and LinkedIn. 20% of respondents said they encountered a worker as yet having the option to sign in subsequent to leaving the organization.

"Its a well-known fact that cloud applications need arrangements added to improve their security; yet to see 20 percent of application clients concede a break by ex-workers is as yet a shockingly high outcome," FlyingPenguin President Davi Ottenheimer said in an announcement. "The genuine story behind the 80 percent previously utilizing cloud applications as of now is that 70 percent concede applications came without organization endorsement. In 2013, associations need arrangements adaptable enough to help the 60 percent with more than four applications as of now being used, and versatile enough to stay aware of the 35 percent who intend to include at any rate four new applications this year."

Almost seventy five percent (72 percent) of the respondents said they want to give outer clients, for example, advisors, with transitory access to the organization's cloud applications, while simply under half (48 percent) of respondents said they are as yet not ready to sign in to cloud applications with a solitary arrangement of certifications.

The review likewise discovered 59 percent of respondents had various on-premise registries with Active Directory being refered to as the most utilized registry (40 percent), trailed by 17 percent who utilize a Lightweight Directory Access Protocol (LDAP) for overseeing client personalities and application get to. Furthermore, 34 percent of respondents asserted that their security model for cloud applications was unique in relation to for on-premise applications versus 45 percent guaranteeing it is the

equivalent.

Here are different security threats found in cloud computing:-

• Network Availability:

The estimation of cloud computing must be acknowledged when your system network and transmission capacity meet your base needs: The cloud must be accessible at whatever point you need it. In the event that it isn't, at that point the outcomes are the same than a refusal of-administration circumstance.

• Cloud Provider Viability:

Since cloud suppliers are moderately new to the business, there are inquiries concerning supplier reasonability and duty. This worry extends when a supplier expects inhabitants to utilize restrictive interfaces, therefore prompting occupant lock-in.

• Legal and Regulatory Compliance:

It might be troublesome or unreasonable to use open mists if the information you have to process is liable to lawful confinements or administrative consistence. While we ought to anticipate that suppliers should fabricate and confirm cloud to address the necessities of controlled markets, accomplishing confirmations might challenge because of the numerous nontechnical variables including the present phase of general cloud information. As best practices for cloud computing include more noteworthy degree, this worry ought to a great extent become an authentic one.

• Transparency

At the point when a cloud supplier does not uncover subtleties of their interior approach or innovation usage, occupants or clients must believe the cloud supplier's security claims. All things considered, occupants and clients require some straightforwardness by suppliers as to supplier cloud security, protection, and how occurrences are overseen.

• Disaster Recovery and Business Continuity

Occupants and clients require certainty that their activities and administrations will proceed if the cloud supplier's generation condition is liable to a calamity.

- Security Incidents

Occupants and clients should be properly educated by the supplier when an incident happens. Clients may require supplier backing to react to review or appraisal discoveries. Additionally, a supplier may not offer adequate help to occupants or clients for settling investigation.

- New Risks, New Vulnerabilities:

There is some worry that cloud computing brings new classes of dangers and vulnerabilities. Despite the fact that we can hypothesize different theoretical new dangers, genuine adventures will to a great extent be an element of a supplier's execution. Albeit all product, equipment, and systems administration gear are liable to uncovering of new vulnerabilities, by applying layered security and thoroughly thought out operational procedures, a cloud might be shielded from basic kinds of assault

regardless of whether a portion of its parts are characteristically helpless.

- Data Loss:

Another genuine risk originates from cloud computing specialist co-ops' potential failure to avoid information misfortune. In our connected world, the vast majority realize that loss of information is inescapable at some point. Nonetheless, this danger is intensified by the sheer measure of information taken care of by cloud computing specialist organizations. There is expanding measure of delicate information transferred to cloud computing firms and this information could become mixed up in any number of ways, including through unplanned cancellation or debasement.

- Data Handling:

Sharing of innovation and assets among various associations consistently represents a hazard to the information being dealt with. Some of the time

servers at cloud computing firms are arranged to work with information from couple of customers. When information from a customer with various necessities is added to the framework, there are numerous things that may turn out badly.

- Account Hijacking:

Capturing of records at cloud computing organizations is another conceivably genuine risk. It is generally workable for approved organization faculty to remotely access cloud information by means of cell phones or remote PCs. "The potential for record seizing, or information commandeering, increments when representatives are getting to touchy data by means of remote stages that don't really have the security components set up that would somehow exist at a workstation PC," notes Tom Caper from Texas based Microsoft Dynamics Partner.

- Insecure application programming interfaces (APIs):

Shaky application programming interfaces (APIs) are another danger to cloud computing. These interfaces offer ways for projects to speak with one another and their security isn't in every case totally ensured. The provisos in security may allow individuals with malevolent aims access to touchy data going through the correspondence channel.

- Denial of Service:

Despite the fact that it doesn't gravely influence trustworthiness of the information put away in cloud computing servers, refusal of administration can incidentally prevent access from securing information to authentic clients.

- Data Breaches:

One of the top dangers to cloud computing is information ruptures. All the PC frameworks associated with the Internet can be gotten to by for all intents and purposes any individual. This uncovered cloud computing specialist organizations to the risk of gifted programmers with malignant goals. In 2012 the quantity of revealed instances of server breaks was more than 200 and they brought about the loss of around 9 million information

records. An ever increasing number of breaks are normal as the quantity of national (and universal, as we've seen with China) underground hacking networks keeps on developing.

- IAAS, SAAS and PAAS each with its own arrangement of issues:

Cloud computing has three unique pathways as examined before: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). Every vulnerabilities that are not completely settled. For example, programming as an administration sends a similar programming utilized in organized and work area situations and engineers still can't seem to create secure coding that will plug escape clauses and make preparations for entrance.

- Privacy, Data Security and information honesty:

Protection was, and stays, one of the central worries in cloud engineering that has not been agreeably settled. One reason is that various nations have various laws concerning security in regard of information put away in servers working in their nation, however the individual to whom that information has a place might be in another nation. A cloud specialist co-op may guarantee customers that information is completely protected yet he might be committed by law to give authorities access to that information whether the customer concurs or not. Another vexing issue is that laws have not been revised to cover all types of information and may consider just messages and instant messages with the end goal of private data. Information, lamentably, isn't given a similar thought as physical property. On the off chance that, by law, information is gotten to, authorities can likewise lay their hands on information of different customers put away on the equivalent hard circle raising danger of inadvertent blow-back.

- Data spilling security:

In a cloud situation information is spilled through the web. On the off chance that it goes through secure "https" channels, information can be said to be protected and secure. In any case, when information streams over open lines, despite the fact that encoded, the parcels can be gotten to. Access to information relies upon the mastery of the programmer in decoding information parcels. Furthermore, since information in the cloud

is gotten to oftentimes, the odds of mistakes can prompt information debasement or unlawful access by meddlers.

• Data classification in the cloud:

Another persistent issue is that staff of the cloud specialist organization approaches information and despite the fact that encoded, such information could without much of a stretch be gotten to and altered.

• Service Level understandings:

Cloud specialist organizations have their own administration level understandings adjusted to fit in with their strategy for activity. These SLAs may not superbly coordinate customer desires as far as security and well-being. There are a lot of persistent, uncertain inquiries, for example, who offers physical and consistent assets and about reviews and appraisals. Is there any instrument set up to defend information in the event of a lockout brought about by legitimate activity against another customer having the equivalent hard circle space? Do cloud specialist organizations have a system set up for guaranteed information demolition on all servers if a customer wishes to suspend administrations? Obviously, the changeless inquiry is about a specialist organization's proceeded with feasibility to be up and accessible consistently. Two or three cloud specialist organizations have collapsed over and clients are naturally worried about security of their information.

As existing issues are tended to and made plans somewhat or even totally, and as cloud administrations extend, up 'til now unexpected issues are probably going to emerge. In the present situation, it is proviso emptor, or let the administration client be amazingly cautious and careful.
Such concerns include the accompanying issues:

1. Leakage and unapproved access of information among virtual machines running on a similar server.

2. Failure of a cloud supplier to appropriately deal with and ensure delicate data.

3. Release of basic and delicate information to law authorization or government organizations without the endorsement and additionally learn-

ing of the customer.

4. Ability to meet consistence and administrative prerequisites.

5. System accidents and disappointments that make the cloud administration inaccessible for broadened timeframes.

6. Hackers breaking into customer applications facilitated on the cloud and gaining and conveying delicate data.

7. The heartiness of the security assurances organized by the cloud supplier.

8. The level of interoperability accessible with the goal that a customer can without much of a stretch move applications among various cloud suppliers and maintain a strategic distance from "lock-in".

Cloud clients ought to likewise be worried about the proceeded with accessibility of their information over significant lots of time and whether a cloud supplier may secretly abuse delicate information for its very own addition.

## III. CLOUD COMPUTING SECURITY SOLUTIONS

There is little uncertainty that the cloud is the way the future for figuring, however the cloud must probably pick up the trust of people in general. Those accountable for nearby establishments can do their part by guaranteeing that their cloud usage are secure as could reasonably be expected.

Here is the rundown of key techniques that could be executed to verify the information in the cloud:

- Recognize and Allocate Value to Properties:

Resources may include antivirus applications, client relationship the board (CRM) or information, bookkeeping; involving individual client subtleties; or framework like facilitated web servers and OS.

- Examine Your Responsibilities:

Among the biggest cloud assurance issues is the peril of ruptures causing burglary or loss of delicate restrictive data. On the off chance that the subtleties spilled are restrictive to your firm, commitment isn't an issue. Still you ought to comprehend where commitment lies if customer disappear out.

- Study Compliance Necessities:

In few markets account and medicinal services are occurrences mechanical guidelines or government build up criteria for how advanced data is overseen, including expressing the degree of security set up. You couldn't be permitted to set up antivirus, or there could be restriction, similar to the information should be kept inside the outskirts of your own country.

- Conclude Your Risk Tolerance:

These fundamental activities all play into this without a doubt to some degree loose, however significant, after advance. The fundamental factor to consider is the cost of making certain security, regardless of whether in the cloud or at your own working environments.

- Create Security Controls into the Agreement:

The maker probably won't be quick to talk about anything, or might not have any desire to grow adaptability to private companies. At any rate, you ought to circumspectly get familiar with the understanding language as it partners with security controls.

- Password security:

Passwords are fundamental segments with regards to security in a cloud establishment. Lamentably, numerous individuals are as yet foolhardy with the passwords, which can unleash devastation in a cloud establishment. Passwords for an essential server should just be known by the individuals who need this data, and they ought to be changed every now and again. Likewise, the individuals who access cloud servers from work areas ought to be instructed how to make solid passwords and the significance of keeping them mystery. The cloud depends on trust, and one broken secret

phrase can break this trust.

- Use Complex Passwords:

All system instruments, from NAS drives to switches to printers, etc must be set up with complex passwords. That infers as a base eight characters, with consolidated case letters, images and letters and no lexicon words or proper names.

- Consider going past passwords:

Plausibility is to utilize a two-level confirmation method. There are number various advances to achieve this, and each offer some unmistakable preferred position. It ought to be noted, notwithstanding, that these validation strategies may cause disappointment; before choosing to utilize one of these alternatives, test it altogether to guarantee that clients will almost certainly get it.

- Encryption:

It is frequently said that some security openings are unavoidable and that any server can be broken. While this point is easy to refute, it can never be totally realized that a specific server is secure. Perhaps the most ideal approaches to counteract the individuals who access a server inappropriately from taking information is to guarantee that it is encoded. Encryption will restrain the harm that should be possible from a break-in, and it can give clients certainty that their information will be secure.

- Log everything:

For end clients, cloud establishments make completing work and getting to data less difficult. On the servers, in any case, there are sure complexities that are unavoidable. Also, the cloud worldview is still generally youthful, and even specialists just have a couple of long stretches of understanding. Along these lines, it very well may be anything but difficult to wind up befuddled when attempting to investigate issues. Solid, predictable logging can help guarantee that issues are settled as fast as would be prudent and help keep the issue from happening again later on.

- Inquire about Safety and Integrity Certifications:

One methods little organizations could cut off mindfulness on organizations' security controls is to ask various confirmations they could have, or look for reference of them at the produces site. By considering only those makes with recorded, certainly solid security systems may evacuate few of the need to examine further.

- Disable Remote Management:

For all intents and purposes all switches have a remote administration instrument, which licenses you sign in to see or alter arrange designs from the Web. To diminish the peril of unapproved pariah openness to your system, you should debilitate remote administration subsequently regulatory occupations can just be conveyed inside the system.

- Use WPA2:

You maybe as of now comprehend that ensuring your Wi-Fi coordinate with WEP encryption is not really much superior to none in any capacity. In any case, the extraordinarily astounding WPA is incredibly in danger to break, explicitly when lexicon based or/and short passphrases are utilized.

- Do not overlook the firewall:

New techniques for verifying systems have turned out to be prevalent as of late, however a compelling firewall is as yet the best cutting edge answer for avoiding unapproved get to. Remote access is vital when running a fruitful cloud usage, and chairmen will need to have the option to get to servers regardless of whether they are away from the workplace. By finding a way to guarantee that the firewall is just permitting as much access as vital, it might be conceivable to fight off malevolent assailants.

- Check out the Cloud Security Alliance Control record:

The CSA has built up a far reaching document itemizing the due steadiness it proposes organizations start when considering moving data and applications into the cloud.

These methodologies are characterized to help the three chief cloud security destinations: Assuring the secrecy, trustworthiness, and accessibility of data assets.

## IV. CONCLUSION

Despite the fact that security and protection benefits in the cloud can be tweaked and overseen by experienced gatherings that can possibly give proficient security the executives and risk appraisal benefits, the issues we've talked about here demonstrate that current security and security arrangements must be basically reexamined concerning their fittingness for mists.

Many cloud computing specialist organizations are solid and they will even give you a high security ensure for your information on cloud yet the truth of the matter is that when an event, for example, information disappointment happens and it influence your online information then you will be compelled to work as per their calendar and presumably be put on a holding up line like numerous other thousand cloud clients, all these to the detriment of your business. At that point, it each of the zeros down to the essentials of information security, if your information is that significant, cloud or not, simply ensure you have a nearby duplicate in your machine just as the reinforcement to be safe.

The same number of organizations move their information to the cloud the information experiences numerous progressions and there are numerous difficulties to defeat as business applications must be re-planned in an unexpected way. The aftereffect of this is information security nearly quits being the essential concern. Accomplishing the necessities for cloud information security involves applying existing security systems and following sound security rehearses. To be powerful, cloud information security relies upon more than basically applying suitable information security methods and countermeasures.

Numerous enhancements in existing arrangements just as increasingly develop and more up to date arrangements are earnestly expected to guarantee that cloud computing advantages are completely acknowledged as its adoption quickens. Cloud computing is still in its early stages, and how the security and protection scene changes will affect its fruitful, across the

board selection.

REFERENCES

[1]. Liu, Y. et al. (2015) 'A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions', Journal of Computing Science and Engineering, 9(3), pp. 119–133. doi: 10.5626/JCSE.2015.9.3.119.

[2]. Musa, F. A. and Sani, S. M. (2016) 'Security Threats and Countermeasures In Cloud Computing', International Research Journal of Electronics & Computer Engineering, 24.

[3]. Popović, K. and Hocenski, Ž. (2016) 'Cloud computing security issues and challenges', Research Gate.

[4]. TagElsir Ahmed Osman, T., babiker, A. A. and Mustafa, N. (2015) 'External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view', IOSR Journal of Computer Engineering Ver. V, 17(2), pp. 2278–661. doi: 10.9790/0661-17259396.

[5]. Takabi, H., Joshi, J. B. D. and Ahn, G.-J. (2010) 'Security and Privacy Challenges in Cloud Computing Environments', IEEE Security & Privacy Magazine, 8(6), pp. 24–31. doi: 10.1109/MSP.2010.186.

[6]. Paul Wooley.et.al.(2011). "Identifying Cloud Computing Security Risks" Capstone Report. University of Oregon Applied Information Management program. pp. 74

[7]. Wayne A. Jansen.et.al.(2011). "Cloud hooks: Security and Privacy Issues in Cloud Computing". 44th Hawaii International Conference on System Sciences. pp.1-8.

[8]. KuiRen.et.al.(2012). "Security Challenges for the Public Cloud". Illinois Institute of Technology.IEEE Press. pp.69 – 73.

[9]. Sychugov, A. A., Akhmetshin, E. M., Grishin, V. M., Shpakova, R. N., & Plotnikov, A. V. (2019). Algorithm determine trust value to the distributed information systems elements. Journal of Mechanical Engineering Research and Developments, 42(2), 6-9. doi:10.26480/jmerd.02.2019.06.09

[10]. Akhmetshin, E. M., Safiullin, M. R. & Elshin, L. A. (2019). Digital Transformation in the Strategic Development of A University. International Journal of Engineering and Advanced Technology, 9(1), 7395-7398. doi:10.35940/ijeat.A3099.109119

[11]. Ibatova, A. Z. (2019). Error analysis of esl learners at tyumen industrial university. Humanities and Social Sciences Reviews, 7(4), 736-741. doi:10.18510/hssr.2019.7494

UNIVERSIDAD
DEL ZULIA

opción
Revista de Ciencias Humanas y Sociales

Año 35, N° 20, (2019)

Esta revista fue editada en formato digital por el personal de la Oficina de Publicaciones Científicas de la Facultad Experimental de Ciencias, Universidad del Zulia.
Maracaibo - Venezuela

**www.luz.edu.ve**

**www.serbi.luz.edu.ve**

**produccioncientifica.luz.edu.ve**