EDITION NO. 1
SEPTEMBRE 2024

FIREWALL

CLOUD OF FIREWALL

| CYBERSECURITY | MATHEMATICS | CURIOSITIES |

LOGARITHMS: BEYOND FORMULAS

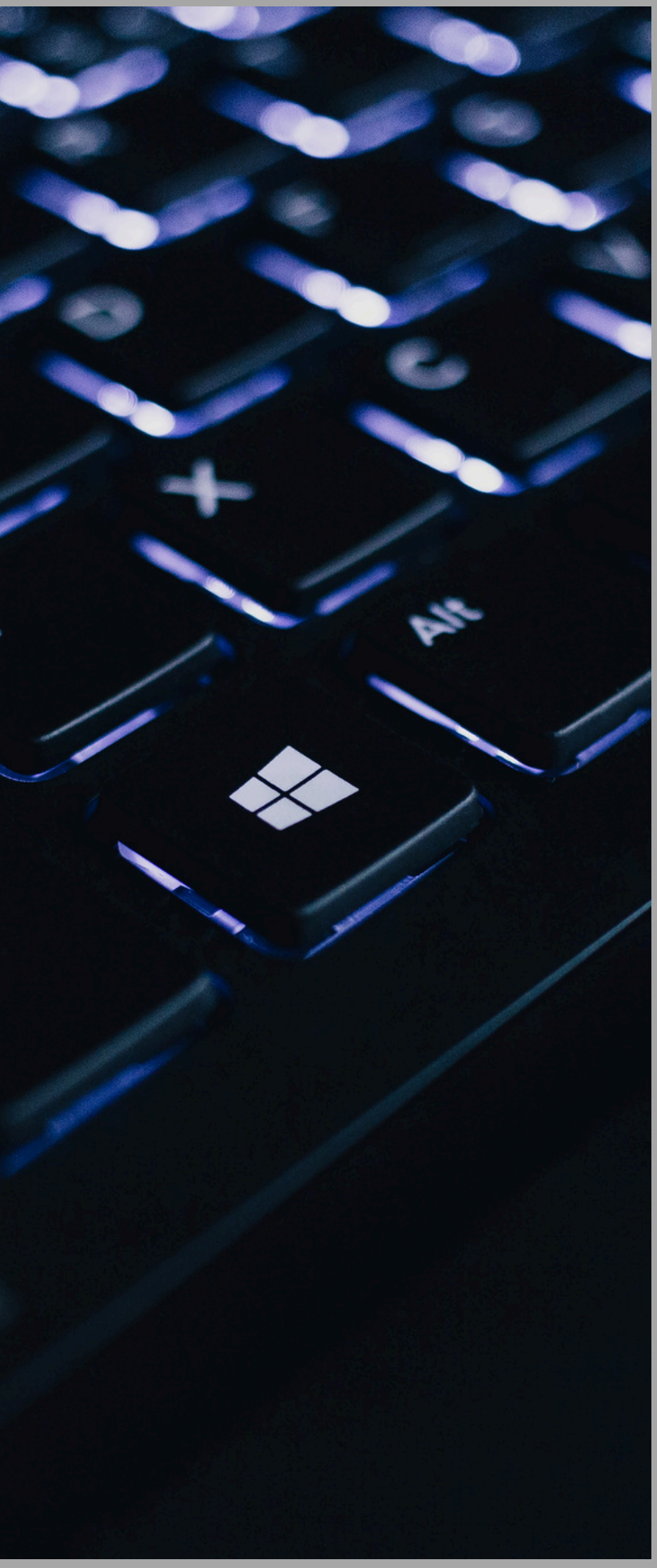
IS AI A DOUBLE-EDGED SWORD ?

8 WAYS TO IMPROVE YOUR CYBERSECURITY

2,00 $

0 65129 43780243

INDEX



CYBERSECURITY: THE VULNERABILITY WE ASSUME IN THE DIGITAL AGE

Today's society is deeply rooted in digital technology, where information travels at the speed of light. From the simplest transactions to the most complex operations, our daily lives increasingly depend on the Internet. But this growing dependence has made us more susceptible to a new type of threat: cyberattacks. These attacks put our privacy and security at risk, stealing information, data or interrupting services.

Cybersecurity is like an invisible shield that protects personal and business information from being stolen or exposed. However, cybercriminals currently have an arsenal of increasingly sophisticated tools, trying to take advantage of people's vulnerabilities to steal data, extort companies and governments or simply cause chaos and disorder. The massive attacks that have affected hospitals, energy companies and even critical infrastructure show that cybersecurity is a national security issue.

Faced with such a threat, it is necessary to adopt a proactive stance, assuming phishing blockers, firewalls, encryption, antivirus, among others. However, cybersecurity is not only the responsibility of companies and governments. Each and every one of us has responsibility. Using strong passwords, not "trusting" suspicious emails, keeping our devices updated are simple measures that can make a big difference.

In short, cybersecurity is a challenge that we all have to face. The time has come to recognize how serious the problem is and to take steps to protect our information and our freedoms. If we do not act proactively, the consequences can be devastating. From the collapse of critical infrastructure to the erosion of trust in institutions, cyberattacks can have a profound impact on our society. It's time to take charge of our digital security.

DIGITAL THREATS AND BUSINESS PROTECTION: XELAR CASE

ISIS S. CEDEÑO- BASTIDAS

ABSTRACT

This article consists of presenting the design proposal of a Digital Cybersecurity Guide for the company Xelar C.A, based on the diagnosis that allowed the detection of the problem regarding the vulnerability of its databases, software and computer security, which could expose it to possible cyber attacks, hacking or network failures. With the digital guide, information and the company's systems will be protected against cyber threats in the company Xelar C.A.

Keywords: Cybersecurity, computer threats, data protection.

RESUMEN

El presente artículo consiste en presentar la propuesta de diseño de una Guía Digital de Ciberseguridad para la empresa Xelar C.A, a partir del diagnóstico que permitió detectar la problemática sobre vulnerabilidad a sus bases de datos, software y seguridad informática, que pudiesen exponerla a posibles ataques cibernéticos, hackeos o caídas de redes. Con la guía digital se logrará proteger información y los sistemas de la empresa contra amenazas cibernéticas en la empresa Xelar C.A.

Palabras claves: Ciberseguridad, amenazas informáticas, protección de datos.

Currently, Venezuela has low attention to Cybersecurity due to an obsolete infrastructure and a shortage of trained professionals in the area, which lead the company to a high risk of vulnerability that translates into monetary losses, customer losses, effective time and electronic equipment. Therefore, the following questions are asked: What would be the procedure to implement Cybersecurity tools? Why is Cybersecurity a process integrated into the business environment? What would be the most common problems that the Xelar company has had? The objectives set are: a) Diagnose the current situation regarding Cybersecurity in the Xelar C.A company located in Barquisimeto, Lara State. b) Identify and classify the strategies and tools for computer security appropriate to the company and c) Design the Digital Guide for Business Cybersecurity. The guide is a tool that will allow to minimize the risk in computer security and will encourage the company to focus on bases for the future and in turn leave a precedent that can be used in any organization that needs it. The guide identifies flaws and weaknesses in Cybersecurity and the steps to follow to prevent an attack and precautions after it.

Among the background, the studies by Rojas and Moreno (2017) entitled Cybersecurity Management and prevention of cyber attacks in SMEs in Peru and Mujica (2016) who carried out the Computer Security Plan for the Universidad Nacional Experimental Politécnica "Antonio José de Sucre" (UNEXPO) are mentioned. Both cases deal with the problem of vulnerability and incidents in computer services that affect private and public companies. The theoretical bases that support the research include the Mosaic Theory in Cybersecurity, which is an advanced approach to the detection and mitigation of cyber threats;

the Information Theory, whose approach studies the processing and measurement of data in the transmission of information; the Siemens Theory, which focuses on people's learning to acquire knowledge in the digital age; and the Security Management Systems and Computer Security Techniques. These foundations allowed us to design a Digital Cybersecurity Guide that can be applied at a business level with the legality supported by articles 49, 57, 60, 102 and 327 of the Constitution of the Bolivarian Republic of Venezuela, which points out the importance of security and protection of information.

This research is descriptive because it focuses on specifically analyzing the computer security problem that currently affects Xelar C.A. The population represents the entire company: facilities, technologies, equipment and human resources; and the intentionally selected sample included 15 people from different departments who will receive induction and training from the digital guide.

The result of the study was the design and development of the Digital Guide on Cybersecurity strategies and tools. The guide was accessible to 51 employees at the company Xelar C.A. who, through training sessions, were provided with the knowledge and skills necessary to protect information and systems against cyber threats, ensuring that they can apply what they have learned in their daily work. In this way, the protection of sensitive data (own and client data) is strengthened, the risk of cyber attacks and their economic consequences (financial losses due to data theft) is reduced, customer confidence is increased (safe handling of information) and the company's reputation is improved, which is reflected in the increase in its sales. The impact is positive by improving its operational efficiency and its strength in the market.

The diagnosis of the current situation revealed cybersecurity problems due to the lack of digital security elements in their computer systems. It is recommended to carry out periodic diagnoses to keep them evaluated and organized. The strategies implemented included making backup copies of documents, implementing antivirus software in each technological resource available in the company, describing malicious emails, improving the choice of passwords, restricting USB ports for the subsequent entry of viruses through flash drives, configuring the system to request authorization for any changes to the equipment and scheduling the execution of antivirus software at the end of each work day. It is recommended to constantly update the implemented strategies and establish a schedule for cleaning equipment, both hardware and software.

The digital guide to cybersecurity strategies and tools for the company Xelar C.A. is an easy-to-use resource that helps the company implement effective security measures, adapted to its needs. The company is recommended to continue carrying out regular training, performing attack simulations so that staff is prepared on how to act during a live attack.

Is AI a Double-Edged Sword ?

Artificial Intelligence (AI) is a branch of computer science that focuses on creating systems and programs capable of performing tasks that normally require human intelligence. These tasks include learning, problem-solving, pattern recognition, decision-making, and understanding natural language.

In the field of cybersecurity, AI plays a crucial role by analyzing and correlating data from events and cyber threats coming from multiple sources. This capability allows large volumes of information to be turned into clear and actionable data, which security professionals use to investigate, respond to, and report on potential attacks. When a cyberattack meets certain criteria defined by the security team, AI can automate the response and isolate the affected resources. Moreover, generative AI takes this process a step further by producing original text in natural language, images, and other content based on existing patterns.

The integration of AI in cybersecurity offers several significant advantages. One of them is the rapid and efficient detection of threats, analyzing large volumes of data in real-time and detecting patterns or anomalies that could indicate a security issue.

Predictive analysis is another major advantage, as AI allows anticipating possible future attacks based on historical data, enabling organizations to prepare and strengthen their defenses in advance.

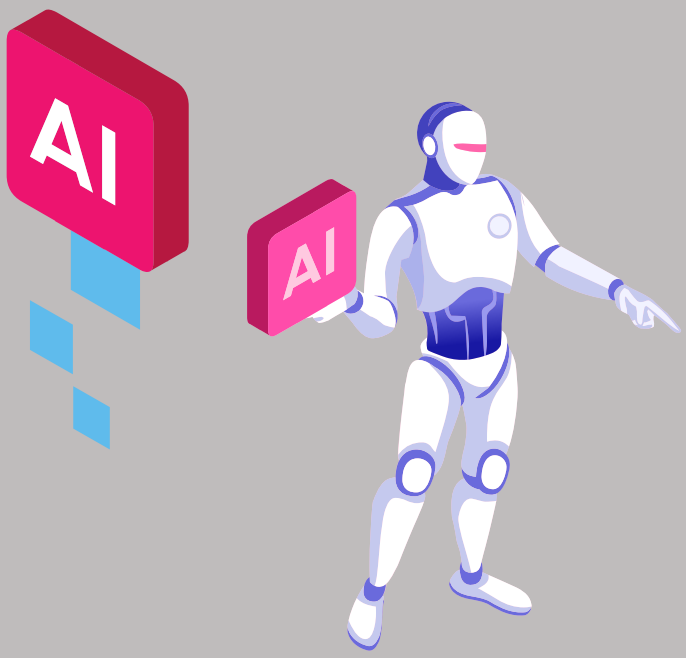
AI-based systems can provide an immediate response to incidents, isolating and mitigating ongoing attacks without the need for human intervention, which significantly reduces response time and potential damage. Additionally, AI algorithms have the ability to continuously improve as they learn from new threats and situations, becoming more effective over time.

"The only limit of AI is human imagination."

-Chris Duffey

However, AI in cybersecurity also presents certain disadvantages. One of them is technological dependency; relying too much on these systems could reduce human oversight, which could be problematic if the AI fails or encounters unforeseen situations. There are also risks of false positives and negatives, where the AI might generate unnecessary alerts or, conversely, fail to detect real attacks, affecting the efficiency and trust in the system. Additionally, cybercriminals can also use AI to enhance the effectiveness of their attacks, developing more sophisticated malware and carrying out more precise and harder-to-detect attacks.

Finally, AI may show rigidity against unknown threats if it is not properly trained or updated, making it less effective against new threats that do not fit into previously known patterns.



Artificial intelligence is therefore a double-edged sword in the field of cybersecurity. While it offers great benefits in threat prevention and risk detection, as well as improving authentication and access control, it also provides cybercriminals with powerful tools to carry out stronger and more impactful attacks. Now, to make the most of the good that AI has to offer and to defend against the threats it poses, organizations must strengthen their defenses and closely monitor incoming threats.

Only the combination of technology and the power of the human mind can be our last hope as we fight against the rising scourge of cybercrime.

"Success in creating AI would be the biggest event in human history. Unfortunately, it could also be the last, unless we learn to avoid the risks."

–Stephen Hawking.

LOGARITHMS: BEYOND FORMULAS

The Power of Simplicity in the world of mathematics, logarithms play a fundamental role that often goes unnoticed. But what exactly is a logarithm? In simple terms, it can be defined as the exponent to which a positive quantity must be raised to obtain a specific number. To understand this better, it is essential to remember that an exponent is the number that indicates the power to which another figure must be raised.

"MATHEMATICS DOESN'T LIE, THERE ARE JUST MANY LYING MATHEMATICIANS."

-Henry David Thoreau (1817-1862)

Applications:

Depending on their use, logarithms can be very beneficial for certain tasks. Let's see in which areas they can be applied:

- **In cybersecurity: They are essential for identifying suspicious or unauthorized activities. By analyzing the logs, specialized cybersecurity personnel can detect intrusion attempts, unauthorized access, and other malicious activities.**
- **In statistics, they are often applied to population growth, especially when the population grows very rapidly (exponentially).**
- **Binary Search: This algorithm, used to find elements in sorted lists, has a complexity. This means that when the size of the list doubles, only a linear increase in the necessary comparisons is required, making it extremely efficient compared to linear search.**

Did you know?

Logarithms are not just theoretical tools; their practical use can simplify complex arithmetic calculations. Instead of performing complicated multiplications or divisions, we can transform these operations into additions and subtractions using logarithms. This property has been fundamental in fields like engineering, science, and economics, where precise calculations are essential.

How to Solve a Logarithm ?

1. The first thing you have to do when you see the equation of the problem is identify the base (b), the exponential expression (x), and the exponent (y). Let's consider an example:

- 5 = log4(1024)
- b = 4
- y = 5
- x = 1024

2. You need to move "x" to one side of the equation, next to the equal sign. According to the example: 1024 = ? Apply the base's exponent by multiplying its value by itself the number of times indicated by the exponent (y). Following the example, it would be 5 times, so 4 * 4 * 4 * 4 * 4 = ?, or it can also be written as 45.

3. In order to solve logarithms, you need to rewrite them as an exponential equation at this point. In this case, it would become 45 = 1024.

4. Perform inverse operations to move any part of the equation that is not part of the logarithm to the other side of the equation.
- Example: log3(x + 5) + 6 = 10
- log3(x + 5) + 6 - 6 = 10 - 6
- log3(x + 5) = 4

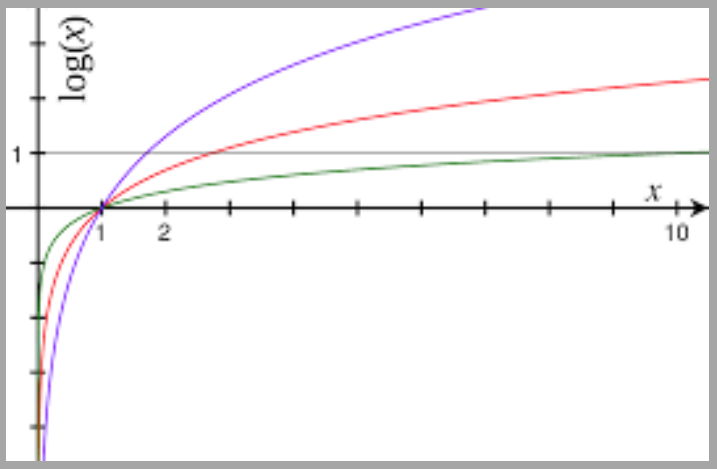
5. Rewrite the equation in exponential form to simplify the logarithm and write the equation in a simpler manner.
Example:

- log3(x + 5) = 4
- Compare this equation with the definition [y = logb (x)] and you can conclude that: y = 4; b = 3; x = x + 5.
- Rewrite the equation to be: by = x
- 34 = x + 5

6. Once you have simplified the problem, solve it as you would with any other equation:

- Example: 34 = x + 5
- 3 * 3 * 3 * 3 = x + 5
- 81 = x + 5
- 81 - 5 = x + 5 - 5
- 76 = x

7. The answer you get in the last step is the solution to the original logarithm, in this case, x = 76.



LET'S SEE THIS EXAMPLE:

$$\log(3)+\log(x-1)=\log(2)+\log(x+1)$$

We add the logarithms on both sides of the equation (multiplying their arguments):

- $\log(3 \cdot (x-1)) = \log(2 \cdot (x+1))$
- $\log(3x-3) = \log(2x+2)$

We set the arguments equal and solve the equation:

- $3x-3 = 2x + 2$
- $3x - 2x = 2 + 3$
- $x = 5$

The solution to the logarithmic equation is x = 5.

8 WAYS TO IMPROVE YOUR CYBERSECURITY

In everyday life, we must always think about digital life mainly because this life has taken control of the era, thus dominating people's actions and making the use of digital devices very common in our daily lives. Thanks to this, people have recently become vulnerable to any hacking, scam, or digital damage that may occur due to lack of information.

The dangers lurk around us without us seeing them. They are hidden in the digital world that has become familiar. Whether at home or in companies, the greatest IT security risk is the human element. That's why hackers try to involve gullible employees in 90 percent of their attacks.

To do this, we can test the following items for digital security:

"Any technology connected to the internet can be hacked."

- Abhijit Naskar

TIPS TO IMPROVE YOUR CYBERSECURITY

- Using a VPN on websites where we connect with people from abroad.
- Reading the privacy information provided by an application or website.
- Regularly backing up data.
- Sharing information about cybersecurity and vulnerabilities related to internet connection.
- Activating two-step authentications on applications like WhatsApp or Telegram.
- Using a secure WiFi connection.
- Using reliable antivirus software that can help detect any threats.
- Regularly changing the password for your WiFi connection.

ALPHABET SOUP

Name: _____

Find the words from the list hidden in the alphabet soup.
Notice that they are written from top to bottom, from left to right and vice versa, and diagonally in both directions.
The words are written from left to right and vice versa, and diagonally in both directions.

p	s	i	m	a	l	w	a	r	e	l	g	y	s	a
h	v	u	l	n	e	r	a	b	i	l	i	t	y	u
i	l	y	o	i	u	a	g	r	l	t	i	p	m	t
s	i	a	f	i	r	e	w	a	l	l	s	o	e	h
h	k	s	o	u	o	i	i	t	t	v	p	n	t	e
i	s	u	r	i	v	i	t	n	a	e	n	n	r	n
n	l	n	l	k	u	m	k	u	r	t	o	t	i	t
g	i	l	t	a	c	i	l	a	a	u	i	r	a	i
t	i	l	m	t	i	l	w	s	t	r	t	o	e	c
e	z	e	l	l	e	m	l	e	u	a	p	j	m	a
n	o	z	i	r	o	x	j	z	c	r	y	a	u	t
t	a	a	t	s	c	h	t	a	a	t	r	n	s	i
o	p	s	n	j	n	s	d	u	q	j	c	c	i	o
b	l	a	q	w	o	i	i	a	r	x	n	r	c	n
t	r	m	k	h	a	c	k	e	r	a	e	s	a	x

Antivirus
Malware
Phishing
Firewall

Ransomware
Trojan
Hacker
encryption

authentication
Botnet
Vpn
vulnerability