EDICIÓN NO. 1
SEPTIEMBRE 2024

NUBE DE FIREWALL

| CIBERSEGURIDAD | MATEMATICAS | CURIOSIDADES |

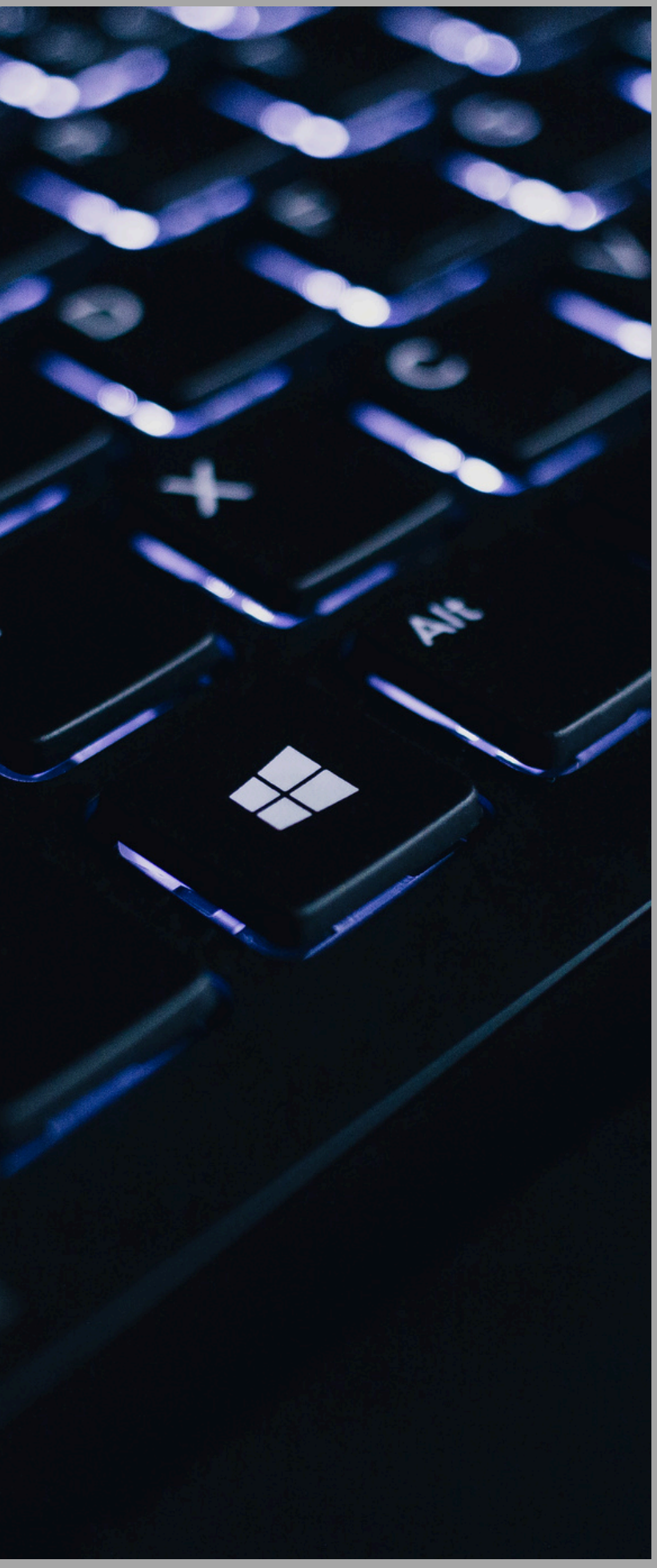
LOGARITMOS: MÁS ALLÁ DE LAS FÓRMULAS

LA IA ¿ UN ARMA DE DOBLE FILO?

8 FORMAS DE MEJORAR TU CIBERSEGURIDAD

2,00 $
0 65129 43780243

ÍNDICE



CIBERSEGURIDAD: LA VULNERABILIDAD QUE ASUMIMOS EN LA ERA DIGITAL

La sociedad actual está profundamente arraigada en la tecnología digital, donde la información viaja a la velocidad de la luz. Desde las transacciones más simples hasta las operaciones más complejas, nuestra vida diaria depende cada vez más de internet. Pero esta creciente dependencia nos ha vuelto más susceptibles a un nuevo tipo de amenaza: los ciberataques, estos ataques ponen en riesgo nuestra privacidad y seguridad, robando información, datos o interrumpiendo servicios.

La ciberseguridad, es como un escudo invisible que protege la información personal y empresarial de ser robada o expuesta. Sin embargo, los cibercriminales actualmente disponen de un arsenal de herramientas cada vez más sofisticadas, intentan aprovechar las vulnerabilidades de las personas para robar datos, extorsionar empresas y gobiernos o simplemente producir caos y desorden. Los ataques masivos que han afectado a hospitales, empresas energéticas e incluso infraestructuras críticas ponen de manifiesto que la ciberseguridad es un asunto de seguridad nacional.

Ante tal amenaza, es necesario adoptar una postura de proactividad, asumiendo bloqueadores de pishing, firewall, encriptaciones, antivirus, entre otros. No obstante, la ciberseguridad no es sólo responsabilidad de las empresas y de los gobiernos. Todos y cada uno de nosotros tenemos responsabilidad. Utilizar contraseñas seguras, no «confiar» en correos sospechosos, mantener nuestros dispositivos actualizados son medidas sencillas que pueden marcar una gran diferencia.

En definitiva, la ciberseguridad es un reto que nos toca afrontar a todos. Ha llegado la hora de reconocer lo serio que es el problema y de adoptar las medidas que sirven para proteger nuestra información y nuestras libertades. Si no actuamos de manera proactiva, las consecuencias pueden ser devastadoras. Desde el colapso de infraestructuras críticas hasta la erosión de la confianza en las instituciones, los ciberataques pueden tener un impacto profundo en nuestra sociedad. Es hora de tomar las riendas de nuestra seguridad digital.

AMENAZAS DIGITALES Y PROTECCIÓN EMPRESARIAL: CASO XELAR.

ISIS S. CEDEÑO- BASTIDAS

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.

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.

INTRODUCCIÓN

Actualmente en Venezuela presenta baja atención en Ciberseguridad dada por una infraestructura obsoleta y escasez de profesionales capacitados en el área, que conllevan a la empresa a un alto riesgo de vulnerabilidad que se traducen en pérdidas monetarias, de clientes, de tiempo efectivo y equipos electrónicos. Por lo consiguiente, se realiza las siguientes interrogantes: ¿Cuál sería el procedimiento para implementar herramientas de Ciberseguridad? ¿Por qué la Ciberseguridad es un procesó integrado al ámbito empresarial? ¿Cuál sería los problemas más comunes que ha tenido la empresa Xelar? Los objetivos planteados son: a) Diagnosticar la situación actual sobre Ciberseguridad en la empresa Xelar C.A ubicada en Barquisimeto, Edo Lara. b) Identificar y clasificar las estrategias y herramientas para la seguridad informática adecuada a la empresa y c) Diseñar la Guía Digital de Ciberseguridad empresarial. La guía es una herramienta que permitirá disminuir al máximo el riesgo en seguridad informática e impulsará a la empresa a centrar bases para el futuro y a su vez dejar un precedente que pueda utilizarse en cualquier organización que la necesite. A través la guía se identifican fallas y debilidades en Ciberseguridad y los pasos a seguir para prevenir un ataque y precauciones posteriores al mismo

Entre los antecedentes se menciona los estudios de Rojas y Moreno (2017) titulado Gestión de la Ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú y Mujica (2016) quien realizó el Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica “Antonio José de Sucre” (UNEXPO). Ambos casos tratan el problema de la vulnerabilidad e incidentes en los servicios informáticos que afectan a empresas privadas y públicas. Las bases teóricas que apoyan la investigación comprende la Teoría del mosaico en la Ciberseguridad el cual es un enfoque avanzado para la detección y mitigación de amenazas cibernéticas; la Teoría de la Información cuyo enfoque estudia el procesamiento y medición de datos en la

transmisión de información; la Teoría Siemens que se centra en el aprendizaje de las personas para adquirir conocimientos en la era digital; y los Sistema de Gestión de Seguridad y Técnicas de Seguridad Informática. Estos fundamentos permitieron diseñar una Guía Digital de Ciberseguridad que puede aplicarse a nivel empresarial con la legalidad soportada en los artículos 49, 57, 60, 102 y 327 de la Constitución de la República Bolivariana de Venezuela que señala la importancia de la seguridad y protección de la información.

La presente investigación es de tipo descriptivo porque se centra en analizar específicamente el problema de seguridad informática que afecta actualmente a Xelar C.A. La población representa la totalidad de la empresa: instalaciones, tecnologías, equipos y recursos humanos; y la muestra seleccionada de manera intencional comprendió 15 personas de diferentes departamentos y quienes recibirán la inducción y capacitación de la guía digital.

El resultado del estudio fue el diseño y elaboración de la Guía Digital sobre estrategias y herramientas de Ciberseguridad. La guía fue de acceso a 51 empleados en la empresa Xelar C.A que mediante sesiones de capacitación fueron dotados de conocimientos y habilidades necesarios para proteger la información y los sistemas contra amenazas cibernéticas, asegurando que puedan aplicar lo aprendido en su trabajo diario. De esta forma se fortalece la protección de datos sensibles (propios y de clientes), se reduce el riesgo de ciberataques y sus consecuencias económicas (pérdidas financieras por robos de datos), aumenta la confianza de los clientes (manejo de información de manera segura) y mejora la reputación de la empresa que se refleja en el incremento de sus ventas. El impacto es positivo al mejorar su eficiencia operativa y su fortaleza en el mercado.

El diagnóstico de la situación actual evidenció los problemas de Ciberseguridad dada la falta de elementos de seguridad digital en sus sistemas informáticos. Se recomienda realizar diagnósticos periódicos para mantenerlos evaluados y organizados. Se implementaron como estrategia la realización de copias de seguridad de documentos, implementación de antivirus en cada recurso tecnológico disponible en la empresa, descripción del correos malicioso, mejorar la elección de contraseñas, restringir los puertos USB para la posterior entrada de virus a través de memorias flash, configuración del sistema para solicitar autorización para cualquier cambios en el equipo y programación de ejecución de antivirus al final de cada jornada laboral. Se recomienda actualización constante de las estrategias implementas y establecer cronograma de limpieza de equipos, tanto de hardware como software.

La guía digital de estrategias y herramientas de Ciberseguridad para la empresa Xelar C.A es un recurso fácil de usar que ayuda a la empresa a implementar medidas de seguridad efectivas, adaptadas a sus necesidades. Se recomienda a la empresa seguir realizando capacitaciones regulares, realizar simulaciones de ataques para el personal esté preparado en cómo actuar mediante un ataque en vivo.

La IA ¿un arma de doblé filo?

La inteligencia artificial (IA) es una rama de la informática que se enfoca en crear sistemas y programas capaces de realizar tareas que normalmente requieren inteligencia humana. Estas tareas incluyen el aprendizaje, la resolución de problemas, el reconocimiento de patrones, la toma de decisiones y la comprensión del lenguaje natural.

En el ámbito de la ciberseguridad, la IA desempeña un papel crucial al analizar y correlacionar datos de eventos y ciberamenazas provenientes de múltiples fuentes. Esta capacidad permite convertir grandes volúmenes de información en datos claros y procesables, que los profesionales de seguridad utilizan para investigar, responder e informar sobre posibles ataques. Cuando un ciberataque cumple con ciertos criterios definidos por el equipo de seguridad, la IA puede automatizar la respuesta y aislar los recursos afectados. Además, la IA generativa lleva este proceso un paso más allá al producir texto original en lenguaje natural, imágenes y otro contenido basado en patrones existentes.

La integración de la IA en la ciberseguridad ofrece varias ventajas significativas, una de ellas es detección rápida y eficiente de amenazas, analizando grandes volúmenes de datos en tiempo real y detectando patrones o anomalías que podrían indicar un problema de seguridad.

El análisis predictivo es otra de las grandes ventajas que sobre la inteligencia artificial ya a que permite anticipar posibles ataques futuros basándose en datos históricos, lo que agiliza en las organizaciones el proceso de preparar y reforzar sus defensas con anticipación.

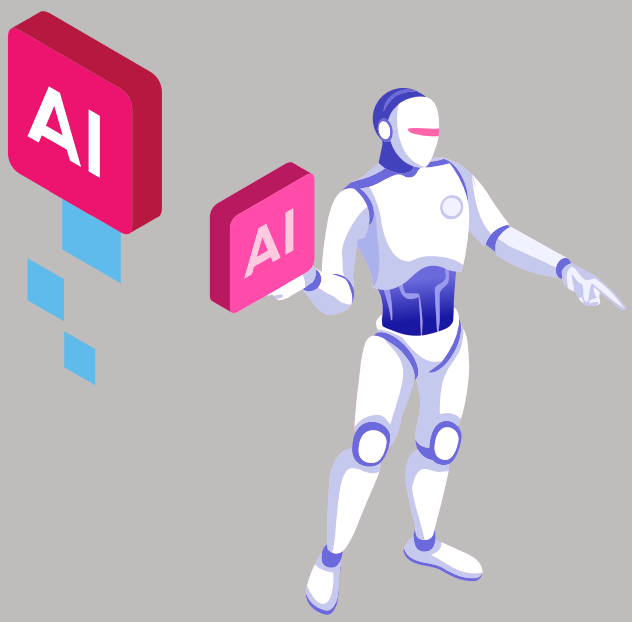
Los sistemas basados en IA pueden ofrecer una respuesta inmediata a incidentes, aislando y mitigando ataques en curso sin necesidad de intervención humana, lo que reduce significativamente el tiempo de respuesta y el potencial daño. Además, los algoritmos de IA tienen la capacidad de mejorar continuamente a medida que aprenden de nuevas amenazas y situaciones, volviéndose más efectivos con el tiempo.

"EL UNICO LIMITE DE LA IA ES LA IMAGINACION HUMANA".

-Chris Duffey

No obstante, la IA en ciberseguridad también presenta ciertas desventajas. Una de ellas es la dependencia tecnológica; confiar demasiado en estos sistemas podría
reducir la supervisión humana, lo que podría ser problemático si la IA falla o enfrenta situaciones imprevistas. También existen riesgos de falsos positivos y negativos, donde la IA podría generar alertas innecesarias o, por el contrario, no detectar ataques reales, afectando la eficiencia y la confianza en el sistema. Además, los ciberdelincuentes también pueden utilizar la IA para mejorar la efectividad de sus ataques, desarrollando malware más sofisticado y llevando a cabo ataques más precisos y difíciles de detectar.

Finalmente, la IA puede mostrar rigidez ante amenazas desconocidas si no está adecuadamente entrenada o actualizada, lo que la hace menos efectiva frente a nuevas amenazas que no encajan en los patrones previamente conocidos.



La inteligencia artificial es, por tanto, un arma de doble filo en el ámbito de la ciberseguridad. Si bien, por un lado, ofrece grandes beneficios en la prevención de amenazas y la detección de riesgos, así como la mejora de la autenticación y el control de acceso; por otro lado, también brinda a los ciberdelincuentes las herramientas de poder para realizar ataques más fuertes e impactantes. Ahora, para sacar el máximo provecho del bien que la IA tiene para ofrecer y para defenderse de las amenazas que plantea, las organizaciones deben endurecer sus defensas y monitorear las amenazas entrantes de cerca.

Solo la combinación de tecnología y el poder de la mente humana podrá ser nuestra última esperanza mientras luchamos contra el flagelo en aumento del cibercrimen.

"El éxito en la creación de IA sería el evento más grande en la historia de la humanidad. Desafortunadamente, también podría ser el último, a menos que aprendamos a evitar los riesgos".

–Stephen Hawking.

LOGARITMOS: MÁS ALLÁ DE LAS FÓRMULAS

La Potencia de la Simplicidad en el mundo de las matemáticas, los logaritmos juegan un papel fundamental que casi siempre pasa desapercibido. Pero, ¿qué es exactamente un logaritmo? En términos sencillos, se puede definir como el exponente al cual se debe elevar una cantidad positiva para obtener un número específico. Para comprenderlo mejor, es esencial recordar que un exponente es el número que indica la potencia a la que debe elevarse otra cifra.

"LAS MATEMÁTICAS NO MIENTEN, LO QUE HAY SON MUCHOS MATEMÁTICOS MENTIROSOS".

Henry David Thoreau (1817-1862)

Aplicaciones:

Dependiendo su uso los logaritmos pueden ser muy beneficiosos para ciertas tareas, veamos en que capo pueden ser aplicados :

·En la ciberseguridad: Son fundamentales para identificar actividades sospechosas o no autorizadas. Analizando los logaritmos, el personal especializado en ciberseguridad puede detectar intentos de intrusión, accesos no autorizados, y otras actividades maliciosas.

·En Estadística se suelen aplicar en el crecimiento de la población, cuando la población crece muy rápidamente (exponencialmente).

·Búsqueda Binaria: Este algoritmo, utilizado para encontrar elementos en listas ordenadas, tiene una complejidad. Esto significa que, al duplicarse el tamaño de la lista, solo se requiere un incremento lineal en las comparaciones necesarias, lo que hace que sea extremadamente eficiente en comparación con la búsqueda lineal.

¿Sabías qué?

¿Los logaritmos no solo son herramientas teóricas? su uso práctico puede simplificar cálculos aritméticos complejos. En lugar de realizar multiplicaciones o divisiones complicadas, podemos transformar estas operaciones en sumas y restas utilizando logaritmos. Esta propiedad ha sido fundamental en campos como la ingeniería, la ciencia y la economía, donde los cálculos precisos son esenciales.

¿ COMO SE RESUELVE UN LOGARTIMO ?

1- Lo primero que tienes que hacer al ver la ecuación del problema es identificar la base (b), la expresión exponencial (x) y el exponente (y). Pongamos un ejemplo:
5 = log4(1024).
b = 4.
y = 5.
x = 1024.

2- Hay que mover "x" a un lado de la ecuación, al lado del signo igual. Según el ejemplo: 1024 =? Aplica el exponente de la base multiplicando su valor por sí mismo la cantidad de veces que indique el exponente (y). Siguiendo el ejemplo, sería 5 veces, por lo tanto 4 * 4 * 4 * 4 * 4 = ?, o también se puede escribir 45.

3- Para poder resolver logaritmos, lo que hay que hacer llegados a este punto es reescribirlos como una ecuación exponencial. En este caso nos quedaría 45 = 1024.

4- Realiza operaciones inversas para mover cualquier parte de la ecuación que no sea parte del logaritmo al otro lado de la ecuación.
Ejemplo: log3(x + 5) + 6 = 10.
log3(x + 5) + 6 – 6 = 10 – 6.
log3(x + 5) = 4.

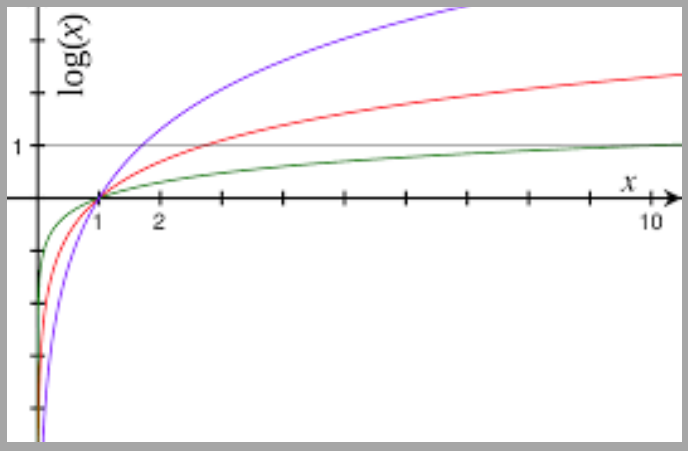
5- Reescribe la ecuación de forma exponencial para poder simplificar el logaritmo y escribir así la ecuación de manera más simple.
Ejemplo:

- log3(x + 5) = 4.
- Compara esta ecuación con la definición [y = logb (x)] y podrás concluir que: y = 4; b = 3; x = x + 5.
- Reescribe la ecuación para que: by = x.
- 34 = x + 5.

6- Cuando ya tengas el problema simplificado, resuélvelo como harías con cualquier otra ecuación:
Ejemplo:

- 34 = x + 5.
- 3 * 3 * 3 * 3 = x + 5.
- 81 = x + 5.
- 81 – 5 = x + 5 – 5.
- 76 = x.

7- La respuesta que obtienes en el último paso es la solución al logaritmo original, en este caso, x = 76.



Veamos este ejemplo:

log(3)+log(x−1)=log(2)+log(x+1)

Sumamos los logaritmos de ambos lados de la igualdad (multiplicando sus argumentos):

- log(3 · (x−1))=log(2 · (x+1))
- log(3x−3)=log(2x+2)

Igualamos los argumentos y resolvemos la ecuación:

- 3x−3=2x+2
- 3x−2x=2+3
- x = 5

La solución de la ecuación logarítmica es x=5

8 MANERAS DE MEJORAR TU CIBERSEGURIDAD

En el día a día siempre debemos pensar en la vida de digital principalmente porque esta vida ha tomado el control de la época dominando así las acciones de las personas y convirtiendo el uso de dispositivos digitales en algo muy común en nuestra vida diaria, gracias a esto últimamente las personas se han vuelto vulnerables a cualquier hakeo, estafa o daño digital que se les presente por la falta de información.

Los peligros nos acechan sin que nosotros los veamos. Están ocultos en el mundo digital que se ha vuelto familiar. Ya sea en casa o en empresas, el mayor riesgo de seguridad de TI es el elemento humano. Es por eso que los piratas informáticos intentan involucrar a empleados crédulos en el 90 por ciento de sus ataques.

Para esto podemos poner a prueba los siguientes ítems para la seguridad digital:

"Ninguna tecnología que esté conectada a Internet es inhackeable"

- Abhijit Naskar

TIPS PARA MEJORAR TU CIBERSEGURIDAD

- **Usar de VPN en páginas donde conectamos con personas del exterior.**
- **Leer las informaciones de privacidad que te ofrece una aplicación o página web.**
- **Realizar copias de seguridad regularmente.**
- **Comparte información sobre la ciberseguridad y la vulnerabilidad que hay con la conexión a internet.**
- **Activar autenticaciones de dos pasos en aplicaciones como WhatsApp o telegram.**
- **Usar una conexión de wifi segura.**
- **Usa antivirus de confianza que puedan ayudar a detectar cualquier amenaza.**
- **Cambia la contraseña de tu conexión a wifi regularmente.**

SOPA DE LETRAS

Nombre: _____

Encuentra las palabras de la lista escondidas en la sopa de letras.
Hay que tener en cuenta que están escritas de arriba a abajo, de izquierda a derecha y viceversa, y en diagonal en ambos sentidos.

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

Antivirus
Malware
Phishing
Firewall

Ransomware
Troyano
Hacker
Cifrado

Auntenticación
Botnet
Vpn
Vulnerabilidad