



# HERRRAMIENTAS DE SEGURIDAD

*Alumno: Alberto Castillo Gómez*

*Grupo: 7 C*

*Fecha: 30/10/2024*

*Docente: Alfredo Pérez Gómez*



# Índice

<b>Índice de ilustraciones .....</b>	<b>2</b>
<b>Índice de tablas .....</b>	<b>3</b>
<b>Introducción .....</b>	<b>4</b>
<b>VirusTotal .....</b>	<b>5</b>
¿Qué es VirusTotal? .....	5
Pruebas realizadas .....	5
<b>Kaspersky password checker .....</b>	<b>8</b>
¿Qué es? .....	8
Pruebas realizadas .....	8
<b>Qualys. SSL Labs .....</b>	<b>11</b>
Pruebas realizadas .....	12
<b>Wapplyzer .....</b>	<b>14</b>
¿Qué es? .....	14
Pruebas realizadas .....	15
<b>¿Cuál es la importancia de la privacidad? .....</b>	<b>18</b>
<b>¿Es necesario un antivirus? .....</b>	<b>18</b>
Sistema Operativo .....	18
Hábitos de Navegación .....	19
Amenazas Comunes .....	19
Protección en Tiempo Real .....	19
<b>¿Cómo navegar de forma segura? .....</b>	<b>20</b>
Brave .....	21
Tor Browser .....	21
Firefox (con extensiones de privacidad) .....	22
DuckDuckGo Privacy Browser .....	22
LibreWolf .....	22
<b>Cliente de correo electrónico seguro .....</b>	<b>23</b>
ProtonMail .....	23
Tutanota .....	23
Mailfence .....	24
Posteo .....	24
StartMail .....	24
<b>Clientes de mensaje instantánea segura y privada .....</b>	<b>25</b>
Signal .....	25
Telegram (Modo Secreto) .....	25
Threema .....	26
Wickr Me .....	26
Element (anteriormente Riot) .....	27
<b>Conclusión .....</b>	<b>29</b>

## Índice de ilustraciones

Ilustración 1 VirusTotal .....	5
Ilustración 2 VirusTotal .....	6
Ilustración 3 VirusTotal .....	6
Ilustración 4 VirusTotal .....	7
Ilustración 5 VirusTotal .....	7

Ilustración 6 VirusTotal .....	7
Ilustración 7 VirusTotal .....	8
Ilustración 8 VirusTotal .....	8
Ilustración 9 KPC .....	9
Ilustración 10 KPC .....	9
Ilustración 11 KPC .....	10
Ilustración 12 KPC .....	10
Ilustración 13 KPC .....	11
Ilustración 14 KPC .....	11
Ilustración 15 SSL Labs .....	12
Ilustración 16 SSL Labs .....	12
Ilustración 17 SSL Labs .....	13
Ilustración 18 SSL Labs .....	13
Ilustración 19 SSL Labs .....	14
Ilustración 20 SSL Labs .....	14
Ilustración 21 Wapplyzer .....	15
Ilustración 22 Wapplyzer .....	15
Ilustración 23 Wapplyzer .....	16
Ilustración 24 Wapplyzer .....	16
Ilustración 25 Wapplyzer .....	17
Ilustración 26 Wapplyzer .....	17
Ilustración 27 Brave .....	21
Ilustración 28 Tor browser .....	21
Ilustración 29 Firefox .....	22
Ilustración 30 DuckDuckGo .....	22
Ilustración 31 LibreWolf .....	23
Ilustración 32 Signal .....	25
Ilustración 33 Telegram .....	26
Ilustración 34 Threema .....	26
Ilustración 35 Wickr Me .....	27
Ilustración 36 Element .....	27

## Índice de tablas

Tabla 1 Comparación de antivirus .....	20
--	----

# Introducción

La seguridad y la privacidad se vuelve un factor importante para las personas cuando sus datos se ven involucrados en herramientas de software para realizar sus tareas diarias. Incluso, cuando las misma empresas se empeñan en proteger la integridad de sus usuarios, no pueden evitar que sus datos sean vulnerados por ataques de terceros.

Para conocer y tomar precauciones al momento de navegar por la web, existen herramientas que pueden ayudar a los usuarios a proteger sus datos y saber lo que hacen durante su navegación. Durante el documento se analizan cuatro diferentes herramientas que te pueden ayudar a revisar la integridad de archivos, sitios web, revisión de contraseñas y el uso de las herramientas dentro de los sitios.

También, se muestran recomendaciones para la navegación segura que van desde el uso de antivirus, clientes de correo electrónico enfocados en la privacidad y seguridad de los usuarios y clientes de mensajería que cumplan con los mismo aspectos.

# VirusTotal

## ¿Qué es VirusTotal?

VirusTotal, que ahora forma parte de Google Cloud, proporciona datos sobre el contexto de las amenazas y sobre reputación para ayudar a analizar archivos, URLs, direcciones IP y dominios sospechosos y poder detectar amenazas de ciberseguridad.

Ahora, se mostrarán 3 pruebas realizadas con la plataforma VirusTotal y como funcionan los principales resultado de cada análisis.

## Pruebas realizadas

El primer elemento analizado es la sitio de descarga de Oracle Virtual Box. Este sitio es un oficial de Oracle y proporciona la fuente principal para la descarga de Virtual Box.

<https://www.virtualbox.org/wiki/Downloads>

Para realizar el análisis de enlaces, se utiliza la herramienta de URL, donde se debe colocar el enlace y presionar la tecla “Enter”.



Ilustración 1 VirusTotal

Cuando se completa el análisis, el primer resultado que se muestra es la cantidad de plataformas que marcan como software malicioso el sitio del enlace. Además, se muestran el

estado en el que se encuentra el sitio, el tipo de contenido, la última fecha de análisis y un pequeño icono que muestra el tipo de software.

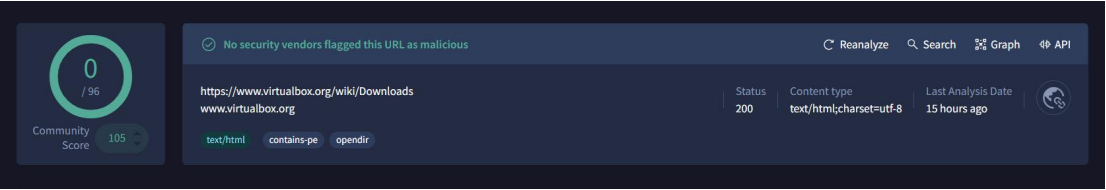


Ilustración 2 VirusTotal

Posterior, se muestran todas las plataformas que han realizado un análisis sobre el software y si este es seguro, es sospechoso o contiene malware.

Security vendors' analysis		Do you want to automate checks?	
ArcSight Threat Intelligence	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AllLabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean

Ilustración 3 VirusTotal

El segundo análisis es para un archivo, es este caso se utiliza la herramienta de “Archivo” donde se puede subir un archivo no mayor a 650MB.



Ilustración 4 VirusTotal

Al igual que en el análisis de URL, se muestra un resumen sobre el archivo analizado pero en este caso se muestra el peso del archivo en lugar del tipo de contenido. También, se pueden mostrar un puntaje dado por la comunidad sobre el software analizado.

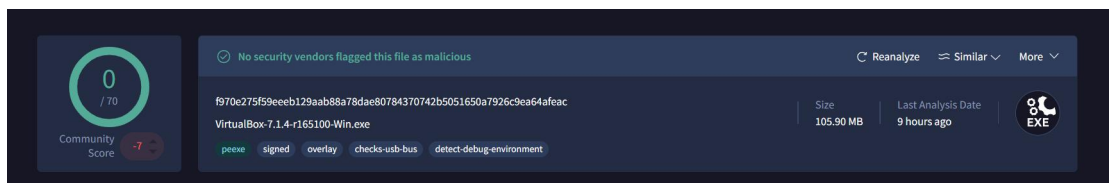


Ilustración 5 VirusTotal

Security vendors' analysis		Do you want to automate checks?	
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AllCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected

Ilustración 6 VirusTotal

El último análisis es sobre el sitio “Elamigos”. Esta plataforma web proporciona miles de video juegos que normalmente solo pueden ser accedidos mediante su compra física o la

adquisición de una licencia. Estos archivos generalmente son vulnerados por la misma por personas con experiencia en desarrollo y son publicados para el acceso de la comunidad. En algunas ocasiones pueden venir con malware integrados dentro de su sistema de archivo.

<https://www.elamigos-games.net/>

En esta ocasión, VirusTotal puede detectar que diferentes plataformas han marcado como malicioso el sitio “Elamigos”, mostrando el tipo de malware que contiene tras su análisis independiente.

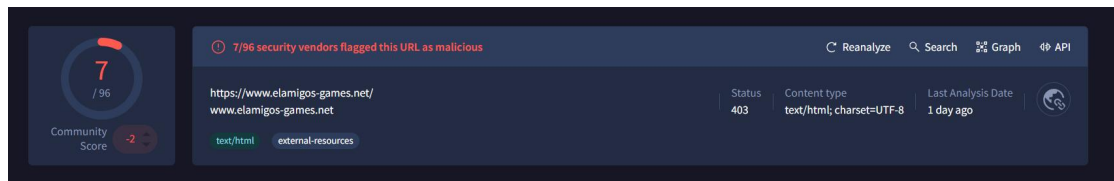


Ilustración 7 VirusTotal

Security vendors' analysis				Do you want to automate checks?	
BitDefender	Phishing	CyRadar	Malicious		
G-Dat	Phishing	Quttera	Malicious		
Seclookup	Malicious	VIPRE	Phishing		
Webroot	Malicious	Abusix	Clean		
Acronis	Clean	ADMINIUSLabs	Clean		
AllLabs (MONITORAPP)	Clean	AlienVault	Clean		
alphaMountain.ai	Clean	Antiy-AVL	Clean		
Artists Against AI	Clean	benkroy.cc	Clean		

Ilustración 8 VirusTotal

## Kaspersky password checker

### ¿Qué es?


Es una herramienta de Kaspersky que permite verificar que tan seguras son las contraseñas que utilizas en diferentes plataformas. KPC permite verificar de una forma sencilla si la contraseña que está analizando puede ser pirateada fácilmente y si esta se encuentra en alguna base de datos de contraseñas filtradas. Adicional a esta información, nos menciona en cuanto tiempo podría ser descifrada la contraseña con un ordenador común.

### Pruebas realizadas

En el siguiente ejemplo, KPC analiza una contraseña implementada dentro de un servicio utilizado de manera personal.





 ¡Buena contraseña!

- Tu contraseña es resistente al pirateo.
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.


Tu contraseña puede ser descifrada con un ordenador común en...

10000+ siglos

Ilustración 9 KPC

Ahora, la siguiente prueba se realiza sobre una contraseña generada de manera automática por LastPass (esta herramienta es un gestor de contraseñas que permite manejar el uso de contraseñas y generar nuevas de manera rápida y sencilla).



 ¡Buena contraseña!

- Tu contraseña es resistente al pirateo.
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.

Tu contraseña puede ser descifrada con un ordenador común en...

4 siglos

Ilustración 10 KPC

Por último, la contraseña analizada no cuenta con caracteres especiales y símbolos por lo que solo esta elaborada con letras en mayúsculas, minúsculas y números.

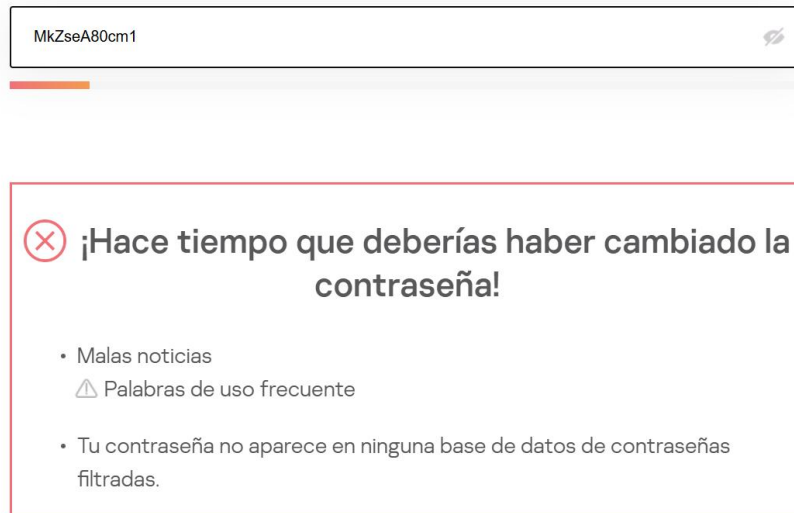


Ilustración 11 KPC

Have I Been Pwned?

¿Qué es?

Have I Been Pwned es un sitio web que permite a los usuarios verificar si sus datos personales han sido comprometidos en una violación de datos.

Para usar HIBP, puedes ingresar una dirección de correo electrónico y ver si se ha visto afectado por una fuga de datos. HIBP mantiene una base de datos sobre contraseñas expuestas y ofrece una API para comprobar una contraseña esta en ella.

En el siguiente ejemplo, se muestra como trabaja HIBP.

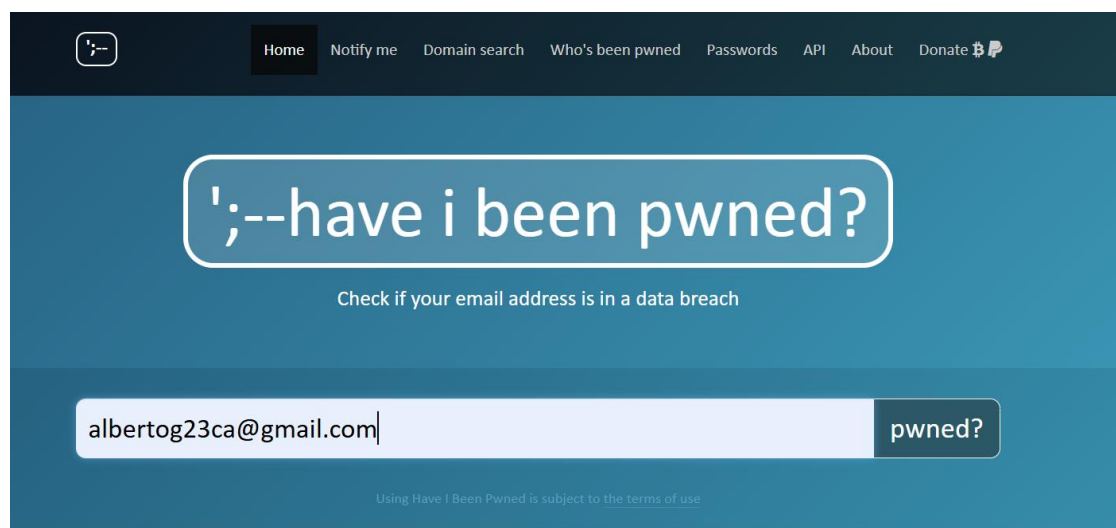


Ilustración 12 KPC

Cuando se realiza el análisis del correo electrónico, arroja los datos encontrados, en este caso HIBP muestra una coincidencia, acompañado de recomendaciones que el mismo sitio te recomienda.

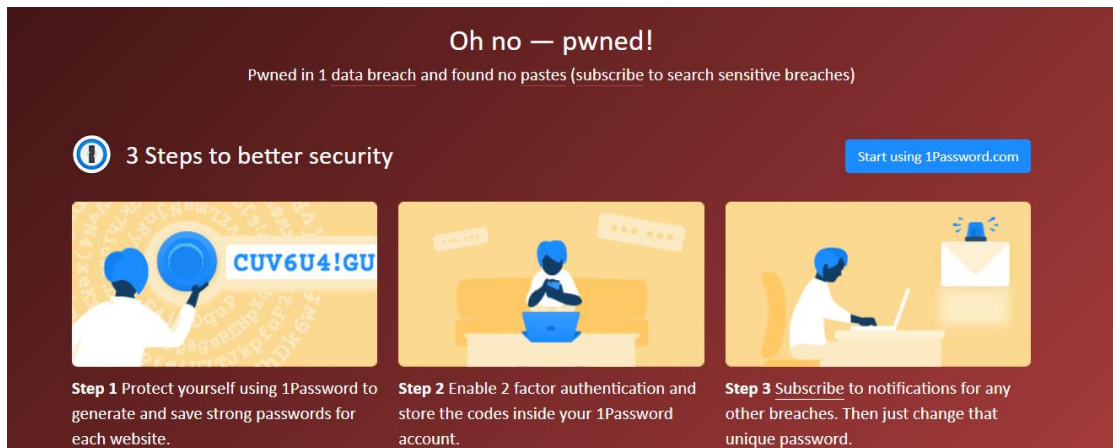


Ilustración 13 KPC

Ahora realizaremos otro análisis.

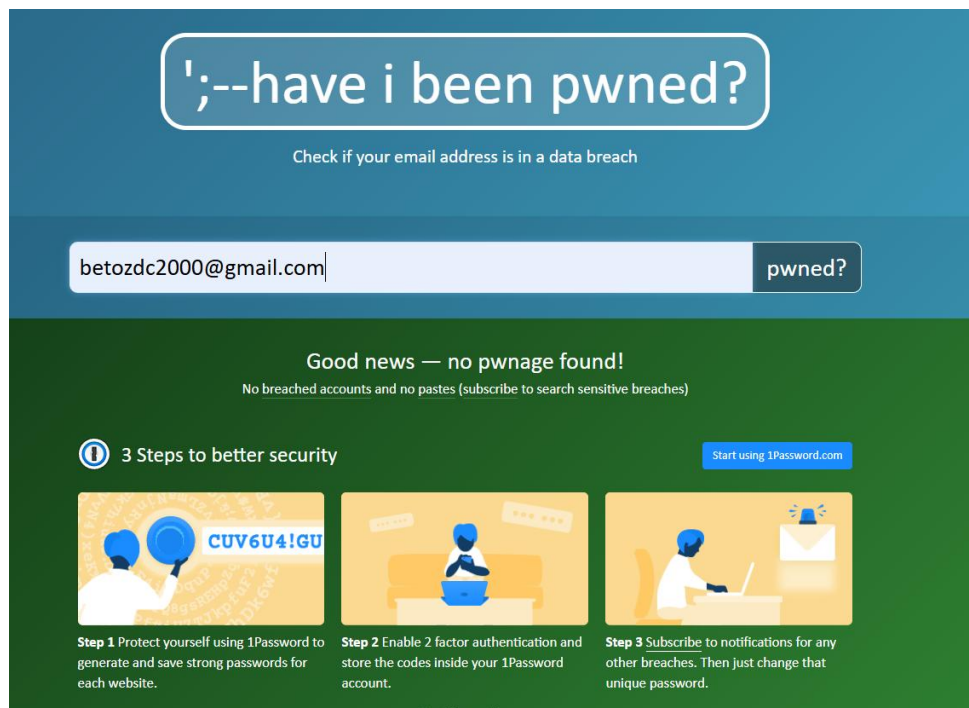


Ilustración 14 KPC

Como podemos ver, no se encontraron coincidencias, por lo que esta dirección de correo no ha sido expuesta dentro de violaciones de datos.

## Qualys. SSL Labs

Es un producto de Qualys que revisa la configuración de seguridad de un sitio web de manera gratuita. SSL Labs es una colección de herramientas, documentos y reflexiones sobre SSL, con el objetivo de comprender mejor cómo se implementa y mejorarlo.

SSL Labs puede detectar si un sitio web puede ser vulnerado por factores como el uso de protocolos inseguros o cifrados obsoletos.

### Pruebas realizadas

A continuación se muestran distintas pruebas dentro de la plataforma de SSL Labs. Para comenzar, se realiza el análisis del sitio oficial de Mercado Libre añadiendo en el enlace del sitio web al formulario.

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Hostname:

https://www.mercadolibre.com.mx/

Submit

☐ Do not show the results on the boards

Ilustración 15 SSL Labs

SSL Report: [www.mercadolibre.com.mx](https://www.mercadolibre.com.mx)

Assessed on: Fri, 25 Oct 2024 01:05:28 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	<a href="#">65.8.161.120</a> server-65-8-161-120.sfo53.r.cloudfront.net Ready	Fri, 25 Oct 2024 01:01:26 UTC Duration: 60.720 sec	A+
2	<a href="#">65.8.161.44</a> server-65-8-161-44.sfo53.r.cloudfront.net Ready	Fri, 25 Oct 2024 01:02:27 UTC Duration: 60.342 sec	A+
3	<a href="#">65.8.161.127</a> server-65-8-161-127.sfo53.r.cloudfront.net Ready	Fri, 25 Oct 2024 01:03:27 UTC Duration: 60.290 sec	A+
4	<a href="#">65.8.161.33</a> server-65-8-161-33.sfo53.r.cloudfront.net Ready	Fri, 25 Oct 2024 01:04:27 UTC Duration: 60.512 sec	A+

SSL Report v2.3.0

Ilustración 16 SSL Labs

Cuando se concluye con el análisis, muestra los resultados en base a las coincidencias.

Ahora, se realiza el análisis de Peña Colorada. <https://www.pcolorada.com/>  
En esta ocasión, el sitio arroja un resumen sobre el análisis de los certificados del sitio, mediante una gráfica de los datos.

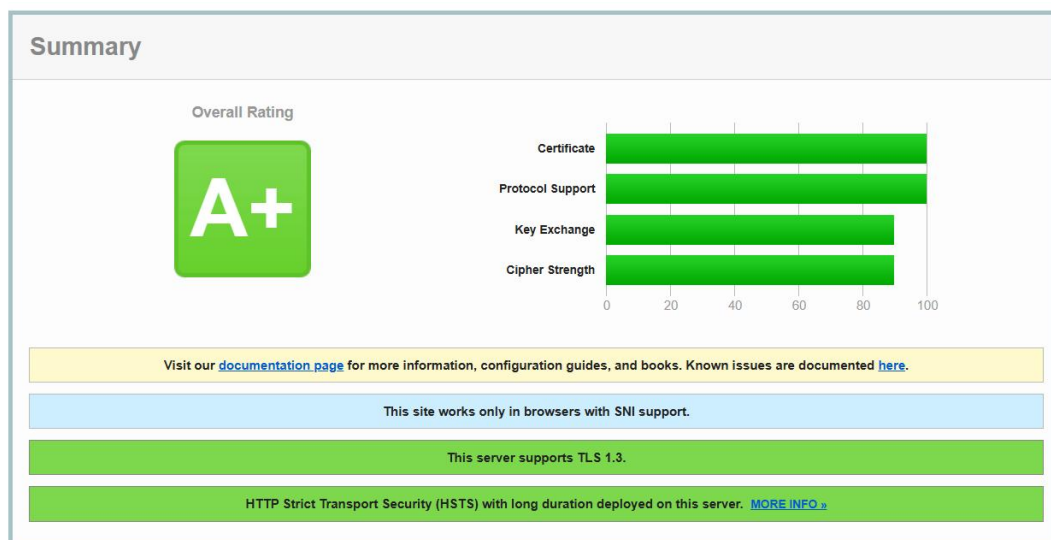


Ilustración 17 SSL Labs

También se muestra los resultado del análisis del certificado del sitio, donde se puede observar información más específica, incluso se extiende bastante la información sobre el sitio de modo que se hace un análisis intenso.

Certificate #1: RSA 2048 bits (SHA256withRSA)	
<div>Server Key and Certificate #1</div>	
Subject	*.pcolorada.com Fingerprint SHA256: edfc2d73b3ae1e16e3b66f895b21ae61c929e4f1944638ab21b002f4788af5a3 Pin SHA256: 5la4mA3i1YG10MXuyuZaxO+zLbXFakl8glm1c63pOY=
Common names	*.pcolorada.com
Alternative names	*.pcolorada.com pcolorada.com
Serial Number	04bc27c41c5a1de5d22c4d2b5ba73e30
Valid from	Thu, 04 Apr 2024 00:00:00 UTC
Valid until	Fri, 04 Apr 2025 23:59:59 UTC (expires in 5 months and 10 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GeoTrust TLS RSA CA G1 AIA: http://cacerts.geotrust.com/GeoTrustTLRSACAG1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://cdp.geotrust.com/GeoTrustTLRSACAG1.crl OCSP: http://status.geotrust.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes

Ilustración 18 SSL Labs

Por último, se hace un análisis sobre el sitio oficial de la Universidad Tecnológica del Valle del Mezquital. <https://www.utvm.edu.mx/>

Este análisis arroja resultados similares al sitio anterior, por lo que segura que los resultado en base al certificado del sitio cuenta con buenas estadísticas.

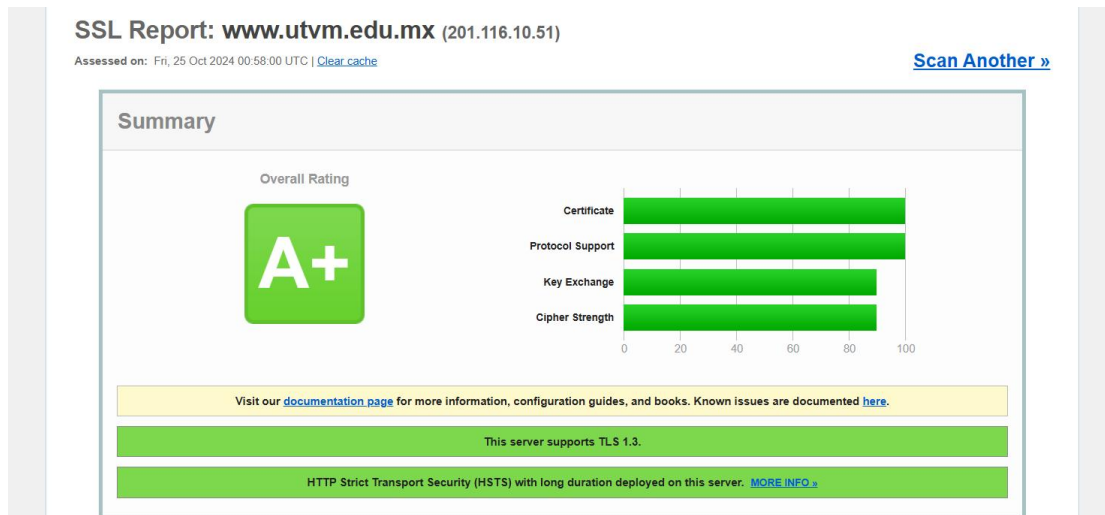


Ilustración 19 SSL Labs

### Certificate #1: RSA 2048 bits (SHA256withRSA)



 <b>Server Key and Certificate #1</b>		
Subject	7citur.utvm.edu.mx Fingerprint: SHA256: 81bd271445d08ee8cfe1c2fb04222f0270e7b393fc2c51feb40759c28a7f4d5f Pin SHA256: 0PEmrzgBuYC3lUKRufZ29AxxQqo1yA5t+liers/kJTU=	
Common names	7citur.utvm.edu.mx	
Alternative names	7citur.utvm.edu.mx www.utvm.edu.mx	
Serial Number	0465b52d8d977105b94419e337eed9970303	
Valid from	Sun, 06 Oct 2024 03:18:07 UTC	
Valid until	Sat, 04 Jan 2025 03:18:06 UTC (expires in 2 months and 10 days)	
Key	RSA 2048 bits (e 65537)	
Weak key (Debian)	No	
Issuer	R11 AIA: <a href="http://r11.o.jencr.org/">http://r11.o.jencr.org/</a>	
Signature algorithm	SHA256withRSA	
Extended Validation	No	
Certificate Transparency	Yes (certificate)	
OCSP Must Staple	No	
Revocation information	OCSP OCSP: <a href="http://r11.o.jencr.org/">http://r11.o.jencr.org/</a>	
Revocation status	Good (not revoked)	
DNS CAA	No (more info)	
Trusted	Yes Mozilla Apple Android Java Windows	

Ilustración 20 SSL Labs

## Wapplyzer

### ¿Qué es?

Wappalyzer es una extensión de navegador que permite descubrir las tecnologías que se utilizan en un sitio web:

- CMS (gestor de contenidos)
- Plataforma de comercio electrónico
- Bibliotecas de JavaScript

- Herramientas de analítica web
- Lenguaje de programación
- Web servers
- Frameworks de JavaScript

Para usar Wappalyzer, se puede instalar la extensión en Chrome o Firefox y hacer clic en el icono de Wappalyzer en la barra de herramientas. Una vez cargados los resultados, la extensión cambiará de color y mostrará una lista de herramientas clasificadas.

## Pruebas realizadas

Para hacer uso de Wappalyzer, debemos instalar la extensión en la tienda de extensiones de Chrome.



Ilustración 21 Wappalyzer

Ahora, para poder hacer uso de la extensión, debemos entrar a un sitio web cualquiera, y hacer clic sobre el icono de “Extensiones” para encontrar la opción de “Wappalyzer - Technology profiler” que nos mostrará las tecnologías implementadas dentro del sitio.

A continuación se muestra una prueba con el sitio oficial de Amazon.  
<https://www.amazon.com.mx/>

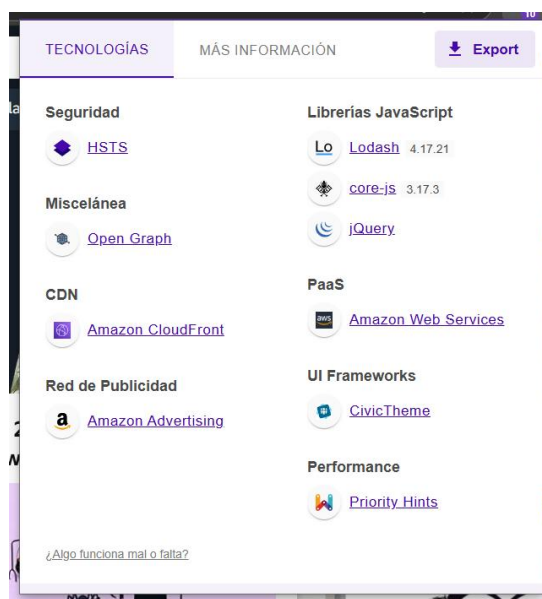


Ilustración 22 Wappalyzer

Aquí se muestran los resultados que arroja la extensión, donde se puede observar que tecnologías se utilizan dentro del sitio. Dichas tecnologías van desde seguridad, librerías, red de publicidad, frameworks, etc.

Ahora, se muestran el resultado de un análisis sobre la página oficial de la UTMV.

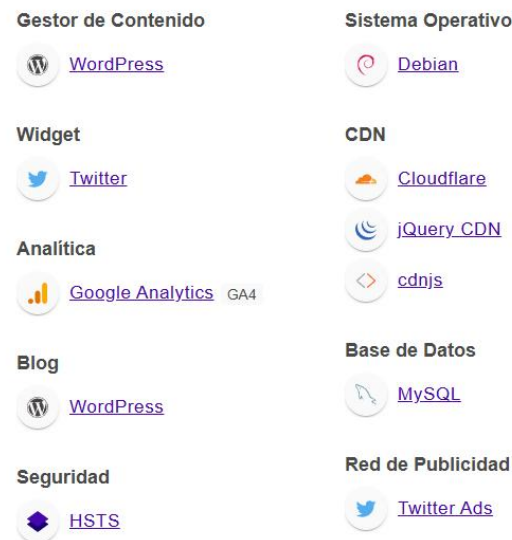


Ilustración 23 Wapplyzer



Ilustración 24 Wapplyzer

Por último, se analiza el sitio de Peña Colorada.
















<b>Gestor de Contenido</b>	<b>Lenguaje de programación</b>
 <a href="#">WordPress</a> 5.7.12	 <a href="#">PHP</a>
<b>Widget</b>	<b>Base de Datos</b>
 <a href="#">Slider Revolution</a> 6.2.8	 <a href="#">MySQL</a>
<b>Galería fotográfica</b>	<b>Tag Manager</b>
 <a href="#">Slider Revolution</a> 6.2.8	 <a href="#">Google Tag Manager</a>
<b>Analítica</b>	<b>Landing Page Builder</b>
 <a href="#">MonsterInsights</a> 8.14.1	 <a href="#">wpBakery</a>
 <a href="#">Google Analytics</a> GA4	<b>SEO</b>
 <a href="#">Facebook Pixel</a> 2.9.174	 <a href="#">Yoast SEO</a>
<b>Blog</b>	 <a href="#">All in One SEO Pack</a>
 <a href="#">WordPress</a> 5.7.12	

Ilustración 25 Wapplyzer




















 <a href="#">WordPress</a> 5.7.12	<b>Librerías JavaScript</b>
<b>Framework JavaScript</b>	 <a href="#">Fancybox</a> 3.1.20
 <a href="#">GSAP</a>	 <a href="#">core-js</a> 2.6.11
<b>Reproductor de Vídeo</b>	 <a href="#">jQuery Migrate</a> 3.3.2
 <a href="#">MediaElement.js</a> 4.2.16	 <a href="#">jQuery</a> 3.5.1
 <a href="#">YouTube</a>	<b>UI Frameworks</b>
<b>Seguridad</b>	 <a href="#">Animate.css</a>
 <a href="#">HSTS</a>	 <a href="#">Bootstrap</a> 4.5.3
<b>Tipografía</b>	<b>WordPress plugins</b>
 <a href="#">Google Font API</a>	 <a href="#">Yoast SEO</a>
 <a href="#">Twitter Emoji (Twemoji)</a> 13.0.1	 <a href="#">All in One SEO Pack</a>
<b>Miscelánea</b>	 <a href="#">wpBakery</a>
 <a href="#">RSS</a>	 <a href="#">Contact Form 7</a> 5.5.3
	 <a href="#">MonsterInsights</a> 8.14.1

Ilustración 26 Wapplyzer

## ¿Cuál es la importancia de la privacidad?

La privacidad es fundamental en la seguridad informática, ya que se refiere a la protección de los datos personales y sensibles de usuarios frente a accesos no autorizados, uso indebido o exposición pública. Aquí algunos puntos clave sobre su importancia:

- **Protección de la Identidad:** La privacidad asegura que la información personal, como nombres, direcciones, y números de identificación, no sea utilizada para robo de identidad.
- **Seguridad Financiera:** Mantener los datos financieros privados evita fraudes y robos, protegiendo cuentas bancarias y tarjetas de crédito.
- **Confidencialidad de la Información:** En las empresas, la privacidad garantiza que datos confidenciales (propiedad intelectual, secretos comerciales) no caigan en manos equivocadas.
- **Cumplimiento Legal:** Existen leyes (como el GDPR en Europa) que obligan a las organizaciones a proteger los datos personales de los usuarios, imponiendo sanciones por violaciones a la privacidad.
- **Prevención de Abuso:** La exposición de datos privados puede llevar a acoso, extorsión, y ataques personalizados, como el phishing.

## ¿Es necesario un antivirus?

La necesidad de un antivirus depende de varios factores, como el sistema operativo que utilizas, tus hábitos de navegación y el nivel de seguridad que buscas en tu equipo. Analizando estos aspectos, podemos determinar cuándo es recomendable tener un antivirus y cuándo podría no ser tan necesario.

### Sistema Operativo

Si utilizas Windows, es importante tener en cuenta que este sistema operativo es uno de los más atacados por malware. Aunque Windows incluye una protección básica con Windows Defender, muchas veces un antivirus de terceros puede ofrecer características adicionales, como protección en tiempo real, defensa contra ransomware o bloqueos de sitios maliciosos. Por lo tanto, en Windows, un antivirus es altamente recomendable para mantener tu equipo seguro.

En el caso de macOS, aunque se considera más seguro que Windows, no está exento de ataques. A medida que crece la popularidad de los dispositivos Apple, los ciberdelincuentes están comenzando a apuntar más a este sistema. Si bien un antivirus no es tan imprescindible como en Windows, sigue siendo una buena idea para protegerte contra

posibles infecciones de malware y para evitar propagar archivos infectados a otros dispositivos.

En cuanto a GNU/Linux, la situación es diferente. Este sistema operativo es menos propenso a ataques debido a su diseño seguro y la baja cantidad de malware dirigido específicamente a él. Sin embargo, si compartes archivos con usuarios de Windows o macOS, puede ser útil tener un antivirus para asegurarte de que no estés distribuyendo archivos infectados, aunque no afecten directamente a tu sistema.

## **Hábitos de Navegación**

Tus hábitos en línea también influyen mucho en la necesidad de un antivirus. Si tiendes a navegar solo por sitios web confiables y descargas software exclusivamente de fuentes verificadas, el riesgo de infección por malware disminuye considerablemente. No obstante, incluso los sitios legítimos pueden verse comprometidos, y siempre existe el riesgo de caer en un ataque de phishing.

Por otro lado, si frecuentemente visitas sitios de descarga de software no verificado, redes P2P o sitios con contenido dudoso, el riesgo aumenta considerablemente. En estos casos, un antivirus se convierte en una herramienta esencial para proteger tu sistema de posibles amenazas.

## **Amenazas Comunes**

Algunas amenazas, como el phishing o los ataques en línea, no siempre dependen directamente del antivirus, pero muchos programas de seguridad incluyen herramientas para bloquear sitios fraudulentos o sospechosos. Además, para amenazas más específicas como el ransomware o los troyanos, los antivirus de pago suelen ser más efectivos, ya que detectan y bloquean este tipo de ataques antes de que puedan comprometer tus archivos o espiar tus actividades.

## **Protección en Tiempo Real**

Una ventaja importante de los antivirus modernos es la protección en tiempo real. Esto significa que escanean automáticamente los archivos que descargas o abres y supervisan tu actividad en línea para detectar posibles amenazas. Este tipo de protección es particularmente útil si tiendes a abrir archivos adjuntos de correos electrónicos de fuentes no verificadas o haces clic en enlaces desconocidos, ya que previene infecciones antes de que lleguen a tu equipo.

Con lo anterior visto, se analizó dos ejemplos de antivirus, uno de ellos de licenciamiento de paga, mientras que el otro es de libre licenciamiento.

Características	Bitdefender Total Security	ClamAV
Plataformas soportadas	Windows, macOS, Android, iOS	Windows, macOS, GNU/Linux, BSD
Protección en tiempo real	Sí	No
Detección de malware	Sí	No
Herramientas de optimización	Sí (limpieza de archivos basura, mejora de rendimiento)	No
Soporte técnico	Soporte 24/7	Comunidad y documentación
Costo	Aproximadamente \$40 - \$60 USD anuales	Gratuito
Compatibilidad con correo electrónico	Sí	Sí

Tabla 1 Comparación de antivirus

## ¿Cómo navegar de forma segura?

Navegar de forma segura implica tomar ciertas precauciones para proteger tus datos, evitar amenazas en línea, y mantener la privacidad en todo momento. A continuación, te doy algunos consejos clave para una navegación segura:

1. Utiliza conexiones seguras (HTTPS): Asegúrate de que los sitios que visitas tengan el protocolo HTTPS, que cifra la información que envías y recibes, protegiéndola de terceros.
2. Actualiza tu navegador y sistema operativo: Mantén siempre tu navegador y tu sistema operativo actualizados para contar con los últimos parches de seguridad.
3. Bloquea anuncios y rastreadores: Los anuncios y rastreadores pueden comprometer tu privacidad. Usa extensiones o navegadores que bloqueen estos elementos automáticamente.
4. Desconfía de correos electrónicos y enlaces sospechosos: No hagas clic en enlaces o descargues archivos adjuntos de correos electrónicos no solicitados, ya que pueden contener malware o llevarte a sitios de phishing.
5. Activa la autenticación de dos factores (2FA): Si es posible, habilita 2FA en tus cuentas para agregar una capa adicional de seguridad en caso de que alguien intente acceder a ellas.

6. No uses redes Wi-Fi públicas sin protección: Si necesitas usar una red Wi-Fi pública, utiliza una VPN para cifrar tu tráfico y evitar que alguien pueda interceptarlo.
7. Gestiona tus contraseñas de forma segura: Utiliza un gestor de contraseñas y crea contraseñas fuertes y únicas para cada cuenta.
8. Deshabilita las cookies de terceros: Configura tu navegador para bloquear cookies de seguimiento y scripts que pueden rastrear tu actividad en línea.

A continuación se muestran 5 navegadores web enfocados en la seguridad y privacidad para los usuarios:

## **Brave**

Brave es conocido por su enfoque en la privacidad y la velocidad. Bloquea anuncios y rastreadores por defecto, permitiendo una navegación rápida y segura. Además, incluye una opción para usar Tor en modo privado, lo que oculta tu IP y cifra tu tráfico para mayor privacidad.



Ilustración 27 Brave

## **Tor Browser**

Tor Browser es uno de los navegadores más seguros para la privacidad. Encripta tu tráfico y lo enruta a través de varios servidores anónimos, haciendo que sea extremadamente difícil rastrear tu actividad en línea. Está diseñado específicamente para la privacidad y el anonimato.



Ilustración 28 Tor browser

## **Firefox (con extensiones de privacidad)**

Firefox es un navegador de código abierto que ofrece buenas características de privacidad, y con algunas configuraciones adicionales (como el uso de extensiones como uBlock Origin, HTTPS Everywhere y NoScript), puede ser una excelente opción para navegar de forma segura.



Ilustración 29 Firefox

## **DuckDuckGo Privacy Browser**

Este navegador móvil, basado en el popular motor de búsqueda DuckDuckGo, prioriza la privacidad bloqueando rastreadores, forzando HTTPS en sitios que lo soportan, y no guarda tu historial de navegación. Es ideal para aquellos que desean una experiencia segura en sus dispositivos móviles.

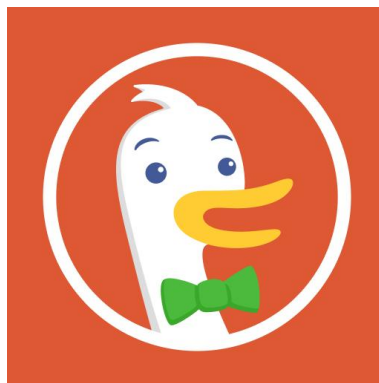


Ilustración 30 DuckDuckGo

## **LibreWolf**

LibreWolf es un fork de Firefox diseñado específicamente para la privacidad y la seguridad. Viene sin telemetría (recolección de datos), y tiene configuraciones de seguridad y privacidad mejoradas, como un mejor bloqueo de rastreadores y cookies.



# Librewolf

Ilustración 31 LibreWolf

## Cliente de correo electrónico seguro

### ProtonMail

Descripción: ProtonMail es uno de los servicios de correo electrónico más populares en cuanto a seguridad. Ofrece cifrado de extremo a extremo para garantizar que solo tú y el destinatario puedan leer los correos. No se requiere información personal para registrarse, y los servidores están ubicados en Suiza, lo que garantiza una mayor protección de datos bajo leyes de privacidad estrictas.

Características destacadas:

- Cifrado de extremo a extremo
- Zero-access (ni siquiera ProtonMail puede leer tus correos)
- Soporte para alias y direcciones personalizadas
- Autenticación de dos factores (2FA)
- Interfaz web y aplicaciones móviles

### Tutanota

Descripción: Tutanota es otra opción que prioriza la privacidad. Al igual que ProtonMail, ofrece cifrado de extremo a extremo y no utiliza publicidad ni recopila datos de los usuarios. Tutanota también cifra los asuntos de los correos y los contactos, brindando una capa extra de privacidad.

Características destacadas:

- Cifrado de extremo a extremo (incluye metadatos y asuntos de correos)
- Aplicaciones para escritorio y dispositivos móviles
- Código abierto y basado en Alemania, bajo las estrictas leyes de privacidad de la UE
- Sin anuncios ni seguimiento
- Opciones gratuitas y premium

## **Mailfence**

Descripción: Mailfence combina seguridad con una suite completa de herramientas de colaboración, como calendarios y almacenamiento de documentos, todo protegido con cifrado OpenPGP. Mailfence te permite controlar tus claves de cifrado, lo que le da una ventaja en términos de control sobre tus datos.

Características destacadas:

- Cifrado OpenPGP (permite gestionar tus claves)
- Compatible con otros servicios de correo electrónico cifrados
- Herramientas integradas (calendario, contactos, documentos)
- Sin anuncios ni rastreo de actividad
- Servidores ubicados en Bélgica, bajo fuertes leyes de privacidad

## **Posteo**

Descripción: Posteo es un servicio de correo electrónico ecológico y seguro con una fuerte política de protección de la privacidad. No requiere información personal para registrarse y permite pagos anónimos. Todos los correos están cifrados en reposo y en tránsito, y Posteo ofrece soporte para la tecnología de cifrado PGP.

Características destacadas:

- Cifrado de extremo a extremo con soporte PGP
- Pagos anónimos (incluso en efectivo)
- Sin anuncios ni rastreadores
- Servidores en Alemania (cumple con el RGPD)
- Interfaz limpia y fácil de usar

## **StartMail**

Descripción: StartMail es un servicio de correo electrónico privado desarrollado por los creadores del motor de búsqueda StartPage. Ofrece cifrado PGP y herramientas fáciles de usar para mejorar la privacidad en tus comunicaciones. StartMail también permite crear direcciones de correo electrónico temporales para mejorar la seguridad en cuentas y registros en línea.

Características destacadas:

- Cifrado OpenPGP (con una configuración fácil para usuarios no técnicos)
- Alias temporales para proteger tu correo real
- Sin anuncios ni recopilación de datos
- Opciones de personalización para alias y dominios personalizados
- Servidores en los Países Bajos, lo que garantiza cumplimiento con el RGPD.



## **Clientes de mensaje instantánea segura y privada**

### **Signal**

Descripción: Signal es ampliamente conocida por su seguridad y privacidad. Ofrece cifrado de extremo a extremo en todos los mensajes, llamadas y videollamadas. Además, no recopila datos personales de los usuarios y permite enviar mensajes que se autodestruyen.

Características destacadas:

Cifrado de extremo a extremo

Código abierto y auditado

Sin recopilación de metadatos

Mensajes autodestructibles

Soporte para autenticación biométrica en dispositivos móviles

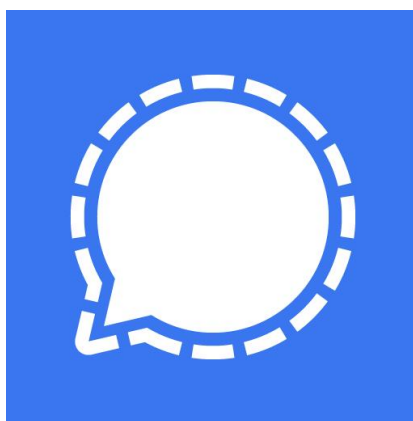


Ilustración 32 Signal

### **Telegram (Modo Secreto)**

Descripción: Telegram ofrece un modo de chat secreto con cifrado de extremo a extremo, y la opción de autodestruir los mensajes después de cierto tiempo. Además, es popular por su amplia gama de funciones y su disponibilidad en múltiples plataformas.

Características destacadas:

Modo de chat secreto con cifrado de extremo a extremo

Mensajes autodestructibles en modo secreto

Opciones avanzadas de personalización

Soporte en múltiples dispositivos

Código parcialmente abierto



Ilustración 33 Telegram

## Threema

Descripción: Threema es una aplicación de pago que prioriza la privacidad. No requiere números de teléfono ni correos electrónicos para registrarse, lo que permite mantener el anonimato. Threema también cifra mensajes, archivos y llamadas de extremo a extremo.

Características destacadas:

No requiere datos personales para el registro

Cifrado de extremo a extremo en mensajes y llamadas

Código abierto y auditado

Servidores en Suiza (fuertes leyes de privacidad)

Opción de mensajes autodestructibles



Ilustración 34 Threema

## Wickr Me

Descripción: Wickr Me es otra aplicación de mensajería privada que utiliza cifrado de extremo a extremo. También permite el anonimato y cuenta con funciones como la autodestrucción de mensajes y la eliminación de metadatos.

Características destacadas:

Cifrado de extremo a extremo en mensajes y archivos

Mensajes que se autodestruyen

No requiere números de teléfono para registrarse

Eliminación de metadatos de archivos compartidos

Modo de anonimato completo



Ilustración 35 Wickr Me

## **Element (anteriormente Riot)**

Descripción: Element es una aplicación de mensajería basada en el protocolo de código abierto Matrix. Está orientada tanto a la privacidad como a la colaboración, y ofrece cifrado de extremo a extremo para mensajes privados y en grupo. Es ideal para quienes buscan una alternativa segura y descentralizada.

Características destacadas:

Cifrado de extremo a extremo

Descentralizado (servidores personalizados)

Código abierto y verificado

Soporte para grupos y colaboración

Compatible con múltiples plataformas

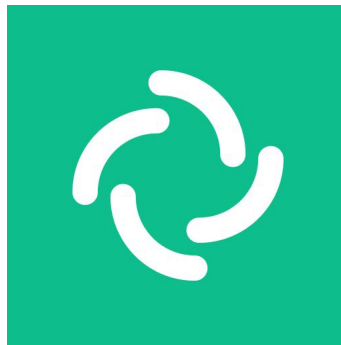


Ilustración 36 Element



## **Conclusión**

En la era digital actual, la navegación segura, la privacidad de la información, y la seguridad en línea son componentes esenciales para proteger nuestra identidad y datos personales. Cada vez que accedemos a Internet, estamos expuestos a diversas amenazas que pueden comprometer nuestra seguridad, desde el robo de información hasta la vigilancia no autorizada. Proteger nuestra información no solo nos ayuda a prevenir ataques cibernéticos y proteger nuestros dispositivos, sino que también asegura nuestra privacidad y autonomía en un mundo cada vez más interconectado.

Utilizar herramientas adecuadas, como navegadores y clientes de correo enfocados en la privacidad, implementar buenas prácticas de seguridad como el uso de contraseñas fuertes y la autenticación de dos factores, y ser conscientes de los riesgos en línea son pasos fundamentales para navegar de manera segura. En conjunto, estas prácticas no solo resguardan nuestra información, sino que también fortalecen el respeto a nuestra privacidad, permitiéndonos una experiencia en línea más confiable y segura.