

Universidad Tecnológica de El Salvador

FACULTAD INFORMÁTICA Y CIENCIAS APLICADAS.

CARRERA TÉCNICO EN INGENIERIA DE HARDWARE.



TEMA: DESARROLLO DE UN KIT DE SEGURIDAD INFORMÁTICA ENFOCADA PARA LA PROTECCIÓN DE LA INFORMACIÓN COMPUTACIONAL TANTO EN HARDWARE COMO EN SOFTWARE PARA LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.

TRABAJO DE GRADUACIÓN PRESENTADO POR:

JORGE ALBERTO ELÍAS CORNEJO.
JAVIER ALEXANDER HERNÁNDEZ HERNÁNDEZ.
ARNOLDO ERNESTO SÁNCHEZ GAMERO.

PARA OPTAR AL GRADO DE:
TÉCNICO EN INGENIERIA DE HARDWARE.

SEPTIEMBRE, 2016.

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA.

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA

VICERRECTOR ACADEMICO

ING. FRANCISCO ARMANDO ZEPEDA

DECANO

JURADO EXAMINADOR

ING. BLADIMIR DÍAZ CAMPOS

PRESIDENTE

ING. HUGO JOEL ORTIZ SALDAÑA

PRIMER VOCAL

ING. MARIO ALBERTO VALLE AGUIRRE

SEGUNDO VOCAL

SEPTIEMBRE, 2016

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA.

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:
Ing. Hugo Joel Ortiz Saldaña, Ing. Mario Alberto Valle Aguirre, Ing. Bladimir Díaz Campos, a las 12:30m. del día Sábado, 25 de Junio de dos mil dieciséis.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

<u>1-Arnoldo Ernesto Sánchez Gamero</u>	<u>Carnet 28-4142-2011</u>
<u>2-Javier Alexander Hernández Hernández</u>	<u>Carnet 28-5738-2013</u>
<u>3-Jorge Alberto Elías Cornejo</u>	<u>Carnet 28-3389-2009</u>

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Desarrollo de un Kit de Seguridad Informática enfocada para la protección de la información computacional tanto en Hardware como en Software para la Universidad Tecnológica de El Salvador"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE HARDWARE

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

Aprobado

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 25 de Junio de dos mil dieciséis.

F. 
PRIMER VOCAL
Ing. Hugo Joel Ortiz Saldaña

F. 
SEGUNDO VOCAL
Ing. Mario Alberto Valle Aguirre

F. 
PRESIDENTE
Ing. Bladimir Díaz Campos

ÍNDICE

Introducción.	i
Capítulo I	1
Planteamiento del problema	1
1. Situación problemática.	1
1.1 enunciado del problema.....	2
1.2 justificación.....	2
1.3 objetivos.	3
1.3.1. objetivo general.	3
1.3.2. objetivos específicos.	3
1.4 delimitaciones.	4
1.4.1 delimitación geográfica.	4
1.4.2 delimitación temporal.	4
1.4.3 delimitación organizacional.	4
1.5. alcances.	6
1.6. Estudio de factibilidad.	7
1.6.1. factibilidad económica.	7
1.6.2. factibilidad técnica.	11
1.6.3. análisis general.....	18
Capítulo II	20
Documentación técnica.	20
1. Marco teórico.	20
1.1. seguridad informática.....	20
1.2. clasificación de seguridad informática.....	20
1.3. herramientas de seguridad.	25
1.4. tipos de amenazas informáticas.	26
1.5. antivirus.	33
1.6. antiespías.	34
1.7. cortafuegos.....	35

1.8. amenazas por internet.....	36
1.9. amenazas en una red inalámbrica o wireless.....	40
1.10. protección informática con cifrado.	43
1.11. seguridad en sistema operativo android.....	44
1.12. disco multimedia.	46
1.13. manual impreso.....	47
1.14. ley especial contra delitos informáticos y conexos.....	48
1.15. ley especial contra actos de terrorismo	49
2. Marco teórico de la solución.	51
2.1. kit de seguridad informática.	51
2.1.1 Ficha técnica de softwares de seguridad informática.....	51
2.1.2 Manual de seguridad informática.	57
2.1.3 manual de instalación y uso de cerradura (applock), para dispositivos Android.	57
2.1.4 manual de instalación y uso adlock plus.	66
2.1.5 .manual de instalación y uso android device manager.	70
2.1.6 manual de instalación y uso de hotspot shield.	75
2.1.7 manual de instalación y uso AVG antivirus.	85
2.1.8 manual de instalación y uso de malwarebytes.	96
2.1.9 manual de instalación y uso de Comodo firewall.....	116
2.1.10 manual de instalación y uso free vpn proxy.....	123
2.1.11 manual de instalación y uso bestcrypt container encryption. ..	126
2.1.12 descripción de DVD multimedia.....	134
3. Marco teórico conceptual.	136
4. Documentación técnica.	144
5. Presupuesto.	159
Capítulo III	160
Desarrollo de la solución.	160
1. Propuesta de la solución.	160

1.1. producto 1, manual de instalación y uso.	163
1.2. producto 2, fichas técnicas.	164
1.3. producto 3, DVD multimedia.	166
2. Conclusiones.	171
3. Recomendaciones.	172
4. Referencias.	174
ANEXO.	179

Introducción.

El siguiente proyecto está basado en la seguridad informática donde la situación problemática se encuentra en los laboratorios de la universidad Tecnológica de El Salvador, específicamente en los equipos informáticos en los cual se pretende dar un mayor rango de seguridad para proteger información personal o privada de virus o software peligrosos que se podrían instalar o ejecutar en los equipos informáticos. En la Universidad Tecnológica de El Salvador se pueden encontrar algunas vulnerabilidades como antivirus desactualizados, virus, malware, etc. que pueden darse por descuido de los administradores o por los mismos estudiantes que instalan software malicioso sin previa autorización son los causantes del robo de información en los laboratorios.

Tomando como referencia estos problemas se plantea la siguiente pregunta:

¿De qué manera se podría proteger la información que manejan los estudiantes dentro de los laboratorios de la Universidad Tecnológica de El Salvador?

Con el desarrollo de este kit se espera que la información que se maneja en los sistemas informáticos sea más segura para los estudiantes y también dar un apoyo a los administradores, para el buen uso y mayor protección de los equipos.

Para ello se investigará los mejores softwares que existan para la seguridad informática, se seleccionarán 3 softwares y se compararán y se seleccionará el mejor evaluado.

Se crearán manuales de cada software que se utilizarán en el kit de seguridad informática, además contará con un DVD multimedia donde estarán recopilados los manuales, contará con softwares de paga Crackeados o parchados solo para fines educativos y algunos videos para instalación de los softwares.

El marco teórico, está enfocado en diferentes temas relacionados a la protección fundamental de la información computacional, para tener una herramienta dirigida a permitir proteger la información privada y confidencial como a la mejor utilización de la herramienta básicamente integrada en un DVD multimedia para ello los planteamos la pregunta.:

¿Qué es la seguridad informática? La seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo.

La seguridad informática se clasifica en: Seguridad física, seguridad lógica, seguridad activa, seguridad pasiva. Dentro de la seguridad informática también existe las amenazas informáticas dentro de los cuales encontramos Virus Informático, ¿Qué es un virus informático? Un virus informático en una definición sencilla y clara es un programa que se copia automáticamente y que tiene como único objetivo que es la de alterar el funcionamiento de la computadora, sin la autorización o el conocimiento del usuario. Entre los daños que pueden ocasionar los virus tenemos: se encuentra el consumo de recursos de un computador, cortes en el sistema de la información o daños a nivel de datos, pérdida de información, etc.

Como combatirlos: La forma más habitual es con un antivirus, pero más que un antivirus este debe estar al día con las actualizaciones de base de datos, ya que por día se crean un aproximado de 30.000 virus, pero aun así con un buen software antivirus que se posea no es garantía de que un virus infecte a una computadora porque los creadores de virus

son demasiados astutos para eso y siempre encuentran una vulnerabilidad para poder afectar los archivos. Dentro de los virus tenemos Spyware, Troyanos (Caballos de toya), Phishing, Spam, Botnets (Zombis), Trashing.

¿Qué es un antivirus? Son herramientas diseñadas para detectar, bloquear y eliminar virus informáticos y otros programas maliciosos.

Existen dos tipos de antivirus:

Antivirus de escritorio: son aquellos que se instalan en el ordenador de forma local y protegen al equipo de ataques llegados a través de Internet y del correo electrónico, así como de dispositivos extraíbles.

Antivirus en línea: son herramientas que no necesitan ser instaladas en nuestro ordenador y se accede a ellos mediante el navegador y solo es necesario disponer de conexión a Internet, además de un navegador actualizado.

Amenazas por Internet. Los peligros por Internet son cada vez más complejos y van en aumento tal es así que los sistemas de seguridad se ven minimizados por la presencia de nuevos virus y personas con un alto conocimiento de Informática capaces de burlar cualquier sistema de seguridad teniendo como lugar de refugio a Internet.

Hacker. Hacker es una persona con conocimientos de electrónica e informática, que prueba y modifica las cosas que tiene entre sus manos y se pasa largas horas pensando en ello.

Dentro de las amenazas también son vulnerables los sistemas operativos Android. ¿Qué es Android? Es un sistema operativo para dispositivos móviles como teléfonos inteligentes, tabletas, TV y otros dispositivos. Basado en el núcleo Linux, es

desarrollado por la Open Handset Alliance, la cual es liderada por Google, usando diversos conjuntos de herramientas de software de código abierto para dispositivos móviles. ¿Qué tipos amenazas afectan en Android actualmente? Las amenazas maliciosas más comunes Android se encuentran: Virus troyanos por SMS., Módulos de privacidad, Exploits para tener acceso de administrador en Smartphone.

¿Qué es un disco interactivo? Un disco interactivo, es aquel CD o DVD que presenta un contenido multimedia, como sonido, texto, imágenes, movimiento, video entre otros, destinado a ser visto especialmente en las PC, y en casos especiales en las computadoras Mac.

¿Qué es un Manual? El manual de usuario es un documento técnico de un determinado sistema que intenta dar asistencia a sus usuarios. Los manuales de usuario generalmente son incluidos a dispositivos electrónicos, hardware de computadora y aplicaciones.

Hoy en día contamos con una ley Especial Contra Delitos Informáticos y Conexos, Con el objetivo de proteger derechos fundamentales como el honor, intimidad, integridad sexual, propiedad intelectual y seguridad pública; la Asamblea Legislativa aprobó, con 70 votos, la Ley Especial contra los Delitos Informáticos y Conexos; la cual abonará a la prevención y sanción de los de los hechos punibles cometidos mediante el uso de las Tecnologías de la Información y Comunicación (TIC), que afecten la imagen de personas naturales o jurídicas.

En el capítulo III, se hace una descripción general de los 3 productos, DVD multimedia, Manual y uso del software y ficha técnica. También se describirá como está compuesto el DVD multimedia, su página inicial, como se distribuye el menú y su estructura, la

información que tendrá al iniciar cada software, también contendrá videos en la cual el usuario podrá guiarse en la instalación de los softwares y como utilizar cada software. El manual estará impreso en páginas de papel bond tamaño carta, con los pasos a seguir para instalar cada uno de los programas, contará con capturas de imagen en orden lógico según su instalación, las fichas técnicas contarán con los requisitos y características, para la instalación previa del programa, así el usuario tendrá una información previa para ver si sus equipos están en la condición para instalar los softwares. Además de contar en formato impreso en papel, los manuales contarán con formato digital creado en PDF, para mayor facilidad del usuario, cabe mencionar que la computadora del usuario debe contar con un software para visualizar archivos PDF.

También se incluyen unas recomendaciones que ayudará al usuario a prevenir riesgo de pérdida o robo de información y evitar daños de hardware a sus dispositivos como por ejemplo a que el usuario evite las descargas de Apps de terceros o páginas desconocidas. Además, se incluyen unas conclusiones que cómo grupo se desarrollaron en base a las investigaciones que se hicieron en los capítulos anteriores. Entre una de ellas se puede mencionar a que este proyecto beneficiará a los laboratorios de la Universidad Tecnológica de El Salvador a la protección y reducir los riesgos de robo de los datos que los estudiantes manipulan en los centros de cómputos y en la universidad.

Capítulo I

Planteamiento del problema.

1.Situación problemática.

Hoy en día las nuevas tecnologías siguen avanzando a pasos agigantados, a través del hardware y de sus nuevas aplicaciones para facilitar la vida diaria de las personas que hacen uso de las tecnologías.

En el salvador se hace uso de una gama de aplicaciones en la que generalmente son niños, jóvenes, adultos que mayormente utilizan estas tecnologías, como redes sociales (Facebook, Twitter, Instagram, WhatsApp) etc., que son las más populares.

Entre las aplicaciones educativas que se utilizan popularmente en El Salvador están Wikipedia, herramientas de Google y sus variantes. La Universidad Tecnológica no se quedan atrás ya que cuenta con sus propias aplicaciones, entre estas está, Portal UTEC, Aulas Virtuales, Inscripción en Línea y las herramientas con las que cuenta Google que son cuentas asignadas a través del carnet a cada uno de los estudiantes como el usuario y código que se les asigna a los docentes, maestros, empleados de la Universidad a través del internet, existe la amenaza como la negligencia del propio personal o de los estudiantes que por descuidos pueden ser afectados los equipos informáticos o en el mayor de los casos hurto de datos privados y de información. (Erb, 2008)

Entre algunos de los problemas que se podrían encontrar en los laboratorios son:

1. Licencias de antivirus desactualizados.
2. Daño de sistemas operativos como malware, virus.
3. Instalación de programas Bloatware.

4. Violación de las políticas de la seguridad por parte de los estudiantes en los laboratorios de informática.
5. Robo de información personal por parte de los estudiantes que dejan sus cuentas abiertas (redes sociales, correos electrónicos o cuentas de otras páginas web).
6. Robo de información utilizando software como Keylogger.
7. Pérdida de información a través de IP, Internet.

1.1 enunciado del problema.

¿De qué manera se podría proteger la información que manejan los estudiantes dentro de los laboratorios de la Universidad Tecnológica de El Salvador?

1.2 justificación.

El proyecto surge de la necesidad de la protección de la información que se manipula en los laboratorios de la Universidad Tecnológica de El Salvador.

Con el desarrollo del Kit de Seguridad Informática se pretende ayudar y reforzar la protección de la información que los estudiantes de la Universidad Tecnológica de El Salvador manejan en sus laboratorios brindando herramientas de seguridad informática y el manejo adecuado de software para la seguridad y la protección de los mismos, para dar un buen uso a los equipos informáticos, además que en El Salvador ya cuenta con una ley contra delitos informáticos que está sujeta a la publicación en el diario oficial de la república para poder aplicar a todos los delitos informáticos y a la protección de toda la información digital como en el Internet, con este kit de seguridad informática se brindará la protección de la información. (Valenzuela & Sosa, 2013)

VENTAJAS.

Las ventajas que se poseen al desarrollo de este proyecto son:

- Ayudar a reducir los delitos informáticos en los laboratorios de la Universidad y a su vez, que estos laboratorios no los utilicen como medios para cometer delitos informáticos a otras personas o instituciones.

-Evitar la instalación de programas sospechosos sin el consentimiento del usuario o administrador.

-Ayudará a los administradores de los laboratorios a que tengan un amplio conocimiento sobre seguridad informática.

1.3 objetivos.

1.3.1.objetivo general.

Desarrollar un kit de seguridad informática para sistemas operativos Windows 7 o superior y Android 4.0 o superior enfocado a la protección de los datos informáticos que puedan ser utilizados por los estudiantes de la Universidad Tecnológica de El Salvador.

1.3.2.objetivos específicos.

1- Crear manual de software de seguridad informática el cual tendrá imágenes y procedimientos para instalar los softwares que estarán en el DVD multimedia.

2- Investigar los mejores softwares que se utilizaran para la seguridad informática analizarlos, instalarlos y comprobar si realmente protege, después de las pruebas crear fichas técnicas con características, requerimientos de instalación y especificaciones.

3- Crear un kit de seguridad informática con los mejores softwares utilizados para la seguridad informática en un DVD multimedia.

1.4 delimitaciones.

1.4.1 delimitación geográfica.

Se realizará en el departamento de San Salvador municipio de San Salvador utilizando un punto de referencia en la Universidad Tecnológica de El Salvador, Calle Arce principal n° 1020.

1.4.2 delimitación temporal.

El proyecto de Kit de Seguridad Informática se realizará en los laboratorios de la Universidad Tecnológica de El Salvador en las fechas comprendidas del 7 marzo de 2016 hasta el 9 de mayo de 2016.

1.4.3 delimitación organizacional.

El trabajo se desarrollará en la Universidad Tecnológica de El Salvador en la Facultad de Informáticas y Ciencias Aplicada.

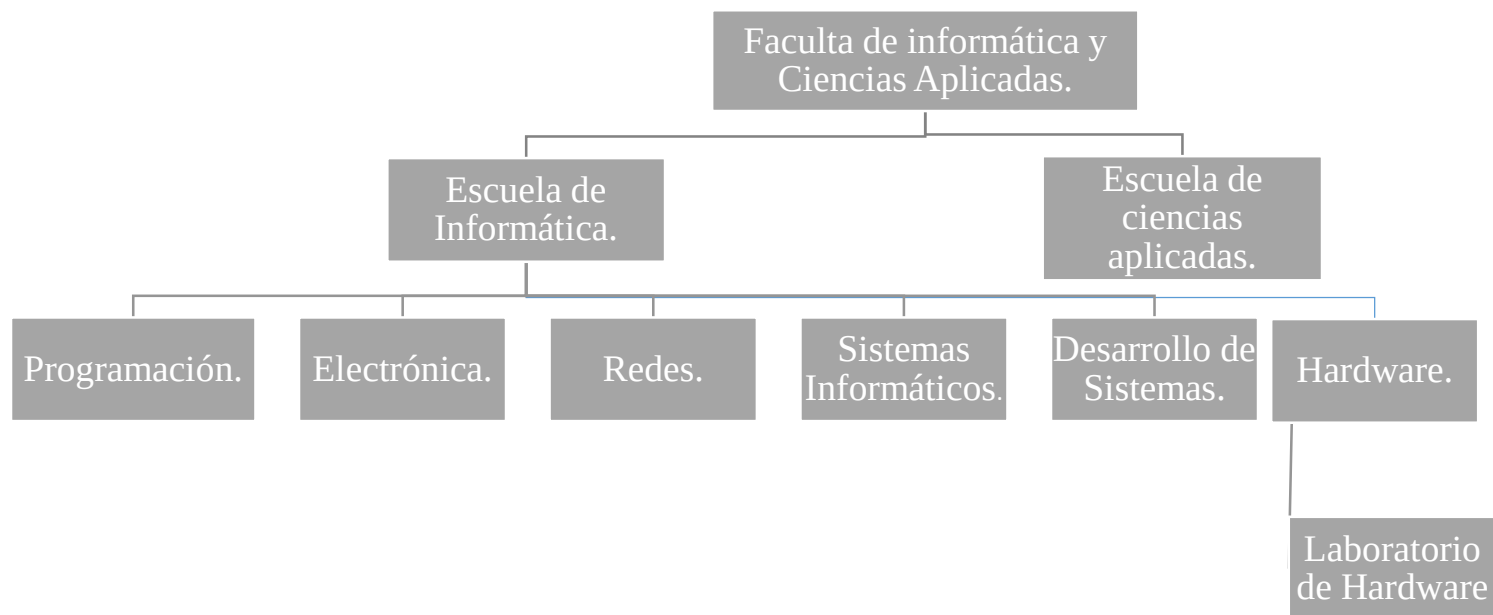


Figura 1, Organigrama.

1.5. alcances.

El desarrollo del siguiente proyecto ofrecerá un Kit de seguridad informática, además incluirá información del software de seguridad informática, estos softwares estarán creados en DVD multimedia, el cual contendrá los programas y manuales para su correcto uso en la Universidad Tecnológica de El Salvador. El objetivo de este proyecto es garantizar la protección de los laboratorios de la Universidad Tecnológica de El Salvador y resolver los problemas de hardware y software que se pueden encontrar en las computadoras, con esto se pretende que los estudiantes tengan a disposición material de apoyo para su aprendizaje y seguridad de su información personal, evitar posibles robos de datos informáticos, ya que la variable humana siempre esta propensa a problemas.

Entre los problemas de software que se podrían presentar son:

- Daños en los sistemas operativos por causa de malware, virus o algún otro software sospechoso.
- Robo de información por dejar cuentas abiertas.
- Modificar de las políticas de las computadoras por parte de los usuarios.

Entre los problemas de hardware que se presentan son:

- Daño en los discos duros por algún virus.
- Utilización de USB con virus sin escaneo con antivirus.

Promesa y producto.

En el siguiente cuadro se presentará las promesas que se dejaron con el desarrollo de kit de seguridad informática, así como también de los productos que se dejaron a beneficio de la Universidad Tecnológica de El Salvador y sus estudiantes.

Tabla 1.
Promesas y productos del proyecto.

Promesa.	Producto.
Crear un manual de seguridad informática.	Manual impreso con información técnica de cómo se utilizará cada software, en su contenido tendrá capturas de pantalla con los pasos a seguir para instalar cada uno de los softwares.
Investigar software que se utilizan en la seguridad informática.	Herramientas de software de seguridad informática con fichas técnicas.
Desarrollar un kit seguridad informática.	Kit de seguridad informática multimedia.

1.6. Estudio de factibilidad.

1.6.1. factibilidad económica.

Tabla 2.
Cuadro de Evaluación Económica Programas de Encriptación de archivos y carpetas.

Cuadro de Evaluación Económica Programas de Encriptación de archivos y carpetas.			
Estudio de Factibilidad Económica.			
Nombre del Producto.	Veracryp.	BestCrypt Container Encryption	7-Zip.
Precios	Gratuito.	\$ 59.95	Gratuito.
Análisis.	Económicamente los programas Veracryp y 7-Zip son factibles para los usuarios, sin embargo, se utilizará la versión de paga BestCrypt Container Encryption con crack solo para fines educativos.		
Establecimiento consultado ó URL.	https://veracrypt.codeplex.com/	https://www.jetico.com/online-shop/shop/index/encrypt	http://www.7-zip.org/

Tabla 3.

Cuadro de Evaluación Económico Apps Protección de Aplicaciones Android.

Cuadro de Evaluación Económico Apps Protección de Aplicaciones Android.			
Estudio de Factibilidad Económica			
Nombre del Producto	Cerradura (AppLock)	LOCX	Cerradura (Smart AppLock)
Precios	Gratuito.	Gratuito.	Gratuito.
Análisis	Las 3 Apps son económicamente factibles por los usuarios por poseer una licencia gratuita.		
Establecimiento consultado ó URL.	https://play.google.com/store/apps/details?id=com.domobile.applock	https://play.google.com/store/apps/details?id=com.cy.ou.privacysecurity	https://play.google.com/store/apps/details?id=com.sp.protector.free

Tabla 4.

Cuadro de evaluación económico de Bloqueadores de Ventanas Emergentes.

Cuadro de Evaluación Económico Bloqueadores de Ventanas Emergentes.			
Estudio de Factibilidad Económica.			
Nombre del Producto.	Adblock Plus.	Ublock Origin.	AdFender.
Precios.	Gratuito.	Gratuito.	Gratuito.
Análisis.	Los 3 son factibles económicamente por que son Free para los usuarios.		
Establecimiento consultado ó URL.	https://adblockplus.org/es/firefox	https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=es	http://www.adfender.com/index.html

Tabla 5.

Cuadro de Evaluación Económico Apps Antirrobo Android.

Cuadro de Evaluación Económico Apps Antirrobo Android.			
Estudio de Factibilidad Económica			
Nombre del Producto	Alarma Antirrobo	Avast Anti-Theft	Android Device Manager
Precios	Gratuito.	Gratuito.	Gratuito.
Análisis	Las 3 aplicaciones son factibles económicamente para los usuarios por poseer licencia gratuita.		
Establecimiento consultado ó URL.	https://play.google.com/store/apps/details?id=com.ralok.antitheftalarm	https://play.google.com/store/apps/details?id=com.avast.android.at_play	https://play.google.com/store/apps/details?id=com.google.android.apps.adm

Tabla 6.

Cuadro de Evaluación Económica Proteger Privacidad en Internet.

Cuadro de Evaluación Económica Proteger Privacidad en Internet.			
Estudio de Factibilidad Económica.			
Nombre del Producto.	TunnelBear.	Hotspot Shield.	Tor.
Precios.	Gratuito.	Gratuito.	Gratuito.
Análisis.	Los 3 son factibles económicamente por que son Free para los usuarios, se utilizará Hotspot Shield, sin embargo, si el usuario desea mayor protección con más características puede usar la versión de paga Hotspot Shield Elite de \$ 19.99 por 6 meses.		
Establecimiento consultado ó URL.	https://www.tunnelbear.com/	https://www.hotspotshield.com/es/	https://www.torproject.org/

Tabla 7

Cuadro de Evaluación Económico Antivirus.

Cuadro de Evaluación Económico Antivirus			
Estudio de Factibilidad Económica			
Nombre del Producto	AVG ANTIVIRUS	AVAST ANTIVIRUS	AVIRA ANTIVIRUS
Precios	Free	Free	Free
Análisis	Económicamente los 3 software evaluados son factibles para el usuario por poseer licencia free.		
Establecimiento consultado ó URL.	http://www.avg.com/w-w-es/homepage	https://www.avast.com/es-ww/windows	http://www.avira.com/es/avira-free-antivirus

Tabla 8.

Cuadro de Evaluación Económico Antispyware.

Cuadro de Evaluación Económico Antispyware.			
Estudio de Factibilidad Económica			
Nombre del Producto	Malwarebytes.	Superantispyware.	Emsisoft Antimalware
Precios.	Free y Premium \$24.95 por un año	Gratuito.	Gratuito.
Análisis	En este caso utilizamos la versión Premium utilizando un crack para fines educativos.		
Establecimiento consultado ó URL.	https://www.malwarebytes.org/	http://www.superantispyware.com/	http://www.emsisoft.com/en/software/antimalware/

Tabla 9.

Cuadro de Evaluación Económico Softwares Firewalls.

Cuadro de Evaluación económico Softwares Firewalls			
Estudio de Factibilidad Económica.			
Característica Técnica	Comodo Firewall	Private Firewall	ZoneAlarm
Precios	Gratuito	Gratuito	\$39.95
Análisis	Económicamente el software Comodo Firewall es el mejor evaluado por poseer licencia gratuita		
Establecimiento Consultado ó URL	https://personalfirewall.comodo.com/	http://www.privacyware.com/personal_firewall.html	http://www.zonealarm.com/#

Tabla 10.

Cuadro de Evaluación Económico Apps Protección en Wifi Públicas Android.

Cuadro de Evaluación Económico Apps Protección en Wifi Públicas Android.			
Estudio de Factibilidad Económica			
Nombre del Producto	CloudVPN	FreeVPN Proxy	SpeedVPN
Precios	Gratuito.	Gratuito.	Gratuito.
Análisis	Económicamente las 3 aplicaciones evaluados son factibles para los usuarios por poseer licencia Gratuita.		
Establecimiento consultado ó URL.	https://play.google.com/store/apps/details?id=net.bypass.vpn	https://play.google.com/store/apps/details?id=com.freevpnintouch	https://play.google.com/store/apps/details?id=us.gospeed.speedvpn

1.6.2. factibilidad técnica.

Tabla 11.

Cuadro de Evaluación Técnica Bloqueadores de Ventanas Emergentes.

Cuadro de Evaluación Bloqueadores de Ventanas Emergentes. SE REQUIERE UN NIVEL DE CALIFICACIÓN DEL 95%.							
Característica Técnica	Ponderación	Adblock Plus.		Ublock Origin.		AdFender.	
		Valor	Total	Valor	Total	Valor	Total
Bloquea todo tipo de anuncios publicitarios en nuestra navegación.	20%	2	40%	2	40%	2	40%
Desactiva el seguimiento y el historial realizado por ciertas páginas web para ofrecer publicidad personalizada.	10%	2	20%	1	10%	1	10%
Bloquea el acceso a determinadas páginas potencialmente peligrosas.	10%	1	10%	2	20%	1	10%
Consumo de memoria y CPU.	20%	2	40%	2	40%	2	40%
Puede leer y crear filtros des archivos hosts.	10%	2	20%	1	10%	0	0%
Es compatible con la mayoría de navegadores.	30%	2	60%	1	30%	2	60%
Total.	100%		190%		150%		160%
	%Final	%/2	95%		75%		80%

Análisis: En la tabla anterior se realizó un análisis de tres programas que son utilizados para bloqueo de páginas emergentes el mejor calificado es Adblock plus porque puede desactivar el seguimiento y el historial realizado por ciertas páginas web para ofrecer publicidad personalizada, puede leer y crear filtros de archivos hosts.

Tabla 12.

Cuadro de Evaluación Técnica Evaluación Encriptación de Archivos y Carpetas.

Cuadro de Evaluación Encriptación de Archivos y Carpetas. SE REQUIERE UN NIVEL DE CALIFICACIÓN DEL 85%.							
Característica Técnica	Ponderación	BestCrypt Container Encryption		Veracryp		7-Zip.	
		Valor	Total	Valor	Total	Valor	Total
Encriptación de archivos y carpetas.	20%	2	40%	1	20%	1	20%
Cifra archivos de sistemas operativos de Windows.	10%	2	20%	1	10%	2	20%
Desempeño en el equipo.	10%	2	20%	1	10%	1	10%
Protege de vulnerabilidad	20%	2	40%	1	20%	2	40%
Soporte de archivos previamente cifrados con la aplicación desfasada TrueCryp.	10%	2	20%	0	0%	0	0%
Protección archivos al subir a internet.	30%	1	30%	1	30%	2	60%
Total.	100%		170%		90%		150%
	%Final	%/2	85%		45%		75%

Análisis: En el anterior cuadro se analizó 3 programas utilizados para encriptar el mejor evaluado es BestCrypt Container Encryption ya que es el que mejor con las características antes mencionadas obteniendo un 85% de aprobación requeridos cumple con Encriptación de archivos y carpetas, Cifra archivos de sistemas operativos de Windows, Soporte de archivos previamente cifrados con la aplicación desfasada TrueCryp. En los cuales obtuvo mayor porcentaje y obtuvo mejor porcentaje.

Tabla 13.

Cuadro de Evaluación Técnica Proteger Privacidad en Internet.

Cuadro de Evaluación Proteger Privacidad en Internet. SE REQUIERE UN NIVEL DE CALIFICACIÓN DEL 85%.							
Característica Técnica	ponderación	TunnelBear.		Hotspot Shield.		Tor.	
		Valor	Total	Valor	Total	Valor	Total
Protege su privacidad al enmascarar su dirección IP.	20%	2	40%	1	20%	1	20%
Es rápido para la navegación.	10%	1	10%	2	20%	1	10%
Proporciona una mayor privacidad y seguridad.	10%	1	10%	1	10%	1	10%
Cifra todo el tráfico de internet	20%	1	20%	2	40%	1	20%
Integridad de los datos	10%	2	20%	2	20%	2	20%
Es fácil de instalar.	30%	2	60%	2	60%	1	30%
Total.	100%		160%		170%		110%
	%Final	%/2	80%		85%		55%

Análisis: En el anterior cuadro se analizaron 3 programas para proteger la privacidad en Internet dentro de los cuales salió mejor evaluado el programa Hotspot Shield con un 85% por poseer mayor protección en seguridad y mejor fluidez o rapidez al navegar, su facilidad de instalación y de usar lo hacen una herramienta eficaz y útil cuando se trata de seguridad en internet, sin embargo, si el usuario desea una mayor protección puede actualizar a la versión de paga de Hotspot Shield Elite el cual posee mayor características que en su versión free.

Tabla 14.

Cuadro de Evaluación Técnica Apps Protección en Wifi públicos Android.

Cuadro de Evaluación Apps Protección en WIFI Públicos Android. SE REQUIERE UN NIVEL DE CALIFICACIÓN DEL 95%							
Característica Técnica	Ponderación	Cloud VPN		FreeVPN Proxy		SpeedVPN	
		Valor	Total	Valor	Total	Valor	Total
No necesita registración.	30%	1	30%	2	60%	2	60%
Conexión con varios servidores.	10%	2	20%	2	20%	1	10%
No requiere que sistema sea roteado.	10%	0	0%	1	10%	2	20%
Conexión rápida con servidor.	20%	2	40%	2	40%	1	20%
Conexión segura en WIFI públicos.	30%	2	60%	2	60%	1	30%
Total.	100%		150%		190%		140%
	% Final.	%/2	75%		95%		70%

Análisis: En la tabla anterior se realizó un estudio y pruebas técnicas de cada aplicación, en la cual salió favorecido la aplicación FreeVPN Proxy ya que además de ser gratuito contaba con más característica y que también su entorno de utilización es fácil para el usuario y no necesita ninguna configuración adicional.

Tabla 15.

Cuadro de Evaluación Técnica Apps Antirrobo Android.

Cuadro de Evaluación Apps Antirrobo Android SE REQUIERE UN NIVEL DE CALIFICACION DEL 85%							
Característica Técnica	Ponderación	Alarma Antirrobo		Avast Anti-Theft		Android Device Manager	
		Valor	Total	Valor	Total	Valor	Total
Borrar información del dispositivo	40%	2	80%	2	80%	2	80%
Detección de ubicación	10%	0	0%	1	10%	2	20%
Ubicación por medio de mapa	20%	0	0%	2	40%	1	20%
Bloquear aparato remotamente	20%	1	20%	1	20%	2	40%
Sonar aparato remotamente.	10%	2	20%	1	10%	1	10%
Total			120%		160%		170%
	% Final.	%/2	60%		80%		85%

Análisis: En la tabla anterior se realizaron pruebas técnicas de cada aplicación, favoreciendo a la aplicación Android Device Manager, el cual no necesita de ninguna instalación ya que ya viene instalado en todos los dispositivos Android.

Tabla 16.
Cuadro de Evaluación Técnica Apps Protección de Aplicaciones Android.

Cuadro de Evaluación Apps Protección de Aplicaciones Android SE REQUIERE UN NIVEL DE CALIFICACIÓN DEL 95%.							
Característica Técnica	ponderación	Cerradura (AppLock)		LOCX		Cerradura (Smart AppLock)	
		Valor	Total	Valor	Total	Valor	Total
Poco Uso de Memoria y Batería	20%	2	40%	2	40%	1	20%
Protección de aplicaciones con contraseña o patrón.	40%	2	80%	2	80%	2	80%
Interfaz fácil para el usuario.	10	1	10%	1	10%	2	20%
Ocultar icono de la aplicación.	10	2	20%	0	0%	1	10%
Widget para bloqueo y desbloqueo,	20%	2	40%	0	0%	1	20%
Total.	100%		190%		130%		150%
	% Final	%/2	95%		65%		75%

Análisis: En la tabla anterior se desarrollaron pruebas técnicas de cada aplicación, resultando favorecida la aplicación Cerradura (AppLock), aparte de ser gratuita contaba con más herramientas para la protección de aplicaciones y además de tener un fácil entorno para el usuario.

Tabla 17.
Cuadro de Evaluación Técnica Antivirus Free.

Cuadro de Evaluación Antivirus Free. SE REQUIERE UN NIVEL DE CALIFICACIÓN DEL 85%.							
Característica Técnica	Ponderación	AVG ANTIVIRUS		AVAST Free Antivirus		AVIRA Antivirus	
		Valor	Total	Valor	Total	Valor	Total
Escaneos periódicos.	20%	2	40%	1	20%	2	40%
Escaneo de correos electrónicos de enviado y recibido.	10%	1	10%	1	10%	1	10%
Capacidad de reparar algunos archivos dañados por virus.	10%	2	20%	1	10%	1	10%
Bóveda de virus en el cual los archivos infectados son guardados.	20%	1	20%	1	20%	1	20%
Área de cuarentena	10%	2	20%	20	20%	1	10%
Fácil instalación.	30%	2	60%	1	30%	1	30%
Total.	100%		170%		110%		120%
	%Final	%/2	85%		55%		60%

Análisis: En el cuadro anterior se analizaron 3 antivirus programas útiles para la protección de pc el programa AVG llego a un porcentaje mayor del 85% requerido para aprobación dentro de las carteristas que salió más evaluado esta Capacidad de reparar algunos archivos dañados por virus, Escaneo de correos electrónicos de enviado y recibido etc.

Tabla 18.
Cuadro de Evaluación Técnica Antispyware.

Cuadro de Evaluación Antispyware SE REQUIERE UN NIVEL DE CALIFICACIÓN DEL 85%							
Característica Técnica	ponderación	Malwarebytes.		Superantispyware.		Emsisoft antimalware	
		Valor	Total	Valor	Total	Valor	Total
Bloqueo de sitios web maliciosos.	20%	2	40%	1	20%	1	20%
Protección tiempo real.	10%	1	10%	1	10%	1	10%
Anti-Rootkit.	10%	2	20%	2	20%	2	20%
Modo análisis rápido.	20%	1	20%	1	20%	2	40%
Programador de análisis y actualización de base de datos.	10%	2	20%	1	10%	1	10%
Eliminación de Malware.	30%	2	60%	1	30%	2	60%
Total.	100%		170%		110%		160%
	%Final	%/2	85%		55%		80%

Análisis: En el cuadro anterior se analizó 3 Antispyware. programas utilizados para la protección de infecciones de toda amenaza de internet para los pc Obteniendo un 85% de aprobación Malwarebytes programa que alcanzo altos porcentajes de avaluación en sus características Protección tiempo real, Anti-Rootkit, Modo análisis rápido etc. Ya que utilizaremos la versión Premium utilizando un crack para fines educativos.

Tabla 19.
Cuadro de Evaluación Técnica Firewalls.

Cuadro de Evaluación Firewalls REQUIERE UN NIVEL DE CALIFICACIÓN DEL 95%							
Característica Técnica	Ponderación	Comodo Firewall.		PrivateFirewall.		ZoneAlarm.	
		Valor	Total	Valor	Total	Valor	Total
Completa protección contra troyanos, rootkits, spyware y hackers	20%	2	40%	2	40%	2	40%
Utilización de pocos recursos del sistema.	40%	2	80%	1	40%	2	80%
Actualización constante y automáticas.	20%	2	40%	2	40%	2	40%
Interfaz Fácil de usar.	10%	2	20%	1	10%	1	10%
Protección en la nube.	10%	1	10%	1	10%	1	10%
Total.	100%		190%		140%		180%
	%Final	%/2	95%		70%		90%

Análisis: En la tabla anterior se desarrollaron pruebas técnicas de cada software resultando favorecida el software Comodo Firewall, que además de poseer una licencia Gratuita consumía pocos recursos del sistema y que también su interfaz resultaba ser muy fácil de utilizar incluso para usuarios amateurs.

1.6.3. análisis general.

Adlock Plus: en económico y técnico es factible ya que cuenta con licencia gratuita y además que cumple con los requisitos técnicos.

BestCrypt Container Encryption: no posee licencia gratuita, pero las características técnicas son factibles para el desarrollo del kit de seguridad informática, se utilizará este software de paga con crack o parche solo para fines educativos.

HotSpot Shield: es factible económicamente ya que cuenta con licencia gratuita, técnicamente también se utilizará la versión gratuita de HotSpot Shield.

Free VPN Proxy: se utilizará la versión gratuita como técnica de FreeVPN Proxy ya que cumple con las características adecuadas para su utilización.

Android Device Manager: se utilizará la versión de gratuita de esta app porque además de ser factible económicamente también es factible técnicamente ya que ya viene instalada por defecto en todos los dispositivos Android además de ser muy intuitivo y de fácil utilización.

Cerradura (AppLock): app factible económicamente y técnicamente ya que cuenta con muchas características además de que no posee publicidad.

Avg antivirus: versión gratuita del Avg que se utilizara ya que posee muchas características y que factiblemente cumple con los requisitos requeridos para el desarrollo de este kit de seguridad informática.

MalwareBytes: se utilizará este software ya que su licencia es gratuita además quedo mejor evaluado en la factibilidad técnica.

Comodo Firewall: por poseer licencia gratuita se utilizará este software además que técnicamente posee la mejor calificación y las mejores características que los demás softwares de firewall.

Capítulo II

Documentación técnica.

1.Marco teórico.

1.1.seguridad informática.

La seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo. (Ochoa Ovalle & Cervantes Sánchez, 2012)

Otra definición más concreta que se le puede dar al concepto de seguridad informática es que son todas aquellas prácticas que se llevan a cabo en un sistema de computación con el único fin de proteger, resguardar su funcionamiento y la información que pueda estar contenido en él. (DefiniciónABC, 2016)

En todo caso no existe ningún método o técnica que permita que la información protegida por un sistema de seguridad informática sea vulnerada y que su información pueda ser extraída por ciberdelincuentes o hackers. (Definicion, 2016)

1.2.clasificación de seguridad informática.

La seguridad informática se puede distinguir entre seguridad física y seguridad lógica, y en dependencia del momento preciso de actuación, se puede distinguir entre seguridad pasiva y seguridad activa, minimizando los daños y efectos que puedan causarle al sistema de computación (RedIRIS, 2002)

Seguridad física.

Es toda aquella seguridad que trata de proteger todo el hardware de un sistema de computación (equipos informáticos, cableado, Routers, Switch, etc.), todas las posibles amenazas naturales como terremotos, tifones, inundaciones, robos, sobre cargas eléctricas, etc. (Tarazona T., 2007)

A continuación, se mencionarán algunas de las principales amenazas y algunos mecanismos para salvaguardarnos de ellas.

Tabla 1.

Seguridad Física Amenazas y Mecanismos de defensa. (infosegur, 2013)

Amenazas.	Mecanismos de defensa.
Incendios	• El inmobiliario del centro de cómputo debe ser ignífugo. • La localización del sistema de cómputo no debe estar donde se majen o almacenen sustancias inflamables o explosivos. • Debe de existir sistemas contra incendio, detectores de humo, extintores, etc., para sofocar el incendio con el menor tiempo posible y así evitar cuantiosas pérdidas.
Inundaciones.	• Evitar la ubicación de los sistemas de cómputos en plantas bajas de edificios para proteger de la entrada de agua superficiales. • Impermeabilizar las ventanas techos y puertas para evitar la entra de agua de plantas superiores.
Robos.	• Medidas para evitar la entrada de personal no autorizado a los centros de cómputo con puertas con seguridad biométricas, cámaras de seguridad, vigilantes.
Señales electromagnéticas.	• Evitar la ubicación en lugares que contengan gran radiación de señales electromagnéticas, porque podrían afectare l correcto funcionamiento de los equipos informáticos del cableado de red. • En caso de que no sea posible evitar la ubicación en zonas con grandes señales electromagnéticas, protegerse de dichas emisiones con el uso de filtros o de cableado especial, si es posible utilizar fibra óptica ya que no es sensible con este tipo de señales.
Apagones.	• Utilizar sistemas de alimentación ininterrumpidas, SAI, que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.

Desastres naturales	• Estar en continuo contacto con organismo que informan sobre sistemas de movimiento sísmicos o sistemas meteorológicos.
---------------------	--

Seguridad Lógica.

La seguridad es la que complementa a la seguridad física, en el cual protege el software de los equipos informáticos, tanto las aplicaciones como los datos de los usuarios de amenazas como robos, pérdidas de datos, entrada de virus informáticos, modificaciones de los datos sin autorización, ataques desde la red, etc. (infosegur, 2013)

A continuación, se proporcionará algunas de las principales amenazas y algunos mecanismos de defensa para la protección de los equipos informáticos.

Tabla 2.

Seguridad Lógica Amenazas y Mecanismos de defensa. (infosegur, 2013)

Amenazas	Mecanismos de defensa.
Robos.	• Cifrar la información almacena para que en caso de robo no sea legible. • Utilizar contraseñas para evitar el acceso a la información. • Utilizar sistemas biométricos (huella dactilar, tarjetas de identificación, etc.)
Pérdida de información.	• Realizar copias de seguridad para poder restaurar la información en caso de pérdida u error. • Uso de sistemas tolerantes a fallos, elección del sistema de ficheros del sistema operativo adecuado. • Uso de un conjunto de discos redundantes para proteger contra la pérdida de datos y proporcionar la recuperación de datos en tiempo real.
Pérdida de integridad en la información.	• Uso del comando del sistema operativo sfc (sistema file checker). • Uso de software de chequeo de equipo.
Entrada de virus.	• Uso de antivirus que eviten que infecten los equipos con software malintencionado.
Ataques desde la red.	• Uso de Firewall, autorizando y auditando las conexiones permitidas. • Software de monitorización. • Servidores proxy, autorizando y auditando las conexiones permitidas.

Modificaciones no autorizadas.	• Cifrado de los documentos en el equipo. • Utilizaciones de contraseñas que no permitan el acceso a la información. • Uso de listas de control de acceso.
--------------------------------	--

Seguridad Activa.

La seguridad activa se podría definir como el conjunto de medidas para prevenir e intentar evitar los daños en los equipos informáticos. (infosegur, 2013)

A continuación, se mencionarán algunas medidas principales de seguridad activa.

Tabla 3.

Seguridad Activa Amenazas y Mecanismos de defensa. (infosegur, 2013)

Amenazas.	Mecanismos de defensa.
Uso de contraseñas.	Previenen el acceso de personas no autorizadas.
Listas de control de acceso.	Previenen el acceso a ficheros de personal no autorizados.
Encriptación.	Evita que personas sin autorización puedan interpretar la información.
Uso de software de seguridad informática.	Previene de virus informáticos y de entradas indeseadas al sistema.
Sistemas de ficheros con tolerancia a fallos	Previene fallos de integridad en caso de apagones de sincronización o comunicación.
Cuotas de disco.	Previene que los usuarios hagan uso indebido de la capacidad de almacenamiento del disco duro.

Seguridad Pasiva.

La seguridad pasiva complementa a la seguridad activa, se podría definir como la encargada de minimizar los efectos que haya causado por algún percance. (infosegur, 2013)

Tabla 4.

Seguridad Pasiva Amenazas y Mecanismos de defensa. (infosegur, 2013)

Técnicas de Seguridad Pasiva.	¿Cómo minimiza?
Conjunto de disco redundantes.	Se puede restaurar la información que no es válida ni consistente.
SAI	Una vez que la energía eléctrica se pierde la batería SAI entra en funcionamiento para proporcionar energía para los equipos por un periodo de tiempo.
Realización de copias de seguridad.	En caso de pérdida de la información se puede realizar una restauración con las copias de seguridad.

En el ámbito informático, la seguridad equivale principalmente a garantizar al usuario:

- Consistencia: Comportarse como se espera que se comporte y mantener su comportamiento sin cambios inesperados.
- Servicio: El sistema debe prestar todos los servicios que ofrece de manera confiable, constante y consistente. (Mojsiejczuk, 2007)
- Protección: Si un programa tiene errores y sufre una caída, no debe afectar a la ejecución de otros procesos. Un programa diseñado expresamente para hacer daño debe tener un impacto mínimo en el sistema. Los segmentos de memoria de un proceso deben ser invisibles e inmodificables para cualquier otro proceso. (Mojsiejczuk, 2007)
- Control de Acceso: Los datos generados por un usuario no deben ser accesibles a otro usuario a menos que así sea específicamente solicitado por su dueño. Soportar diferentes modos de acceso a un archivo, de modo que el sistema pueda exigir que un archivo pueda ser leído, pero no ejecutado o abierto para escritura. Los mecanismos de control de acceso deben ser tan granulares como sea posible. (Mojsiejczuk, 2007)
- Autenticación: El sistema debe poseer los mecanismos necesarios para asegurarse que un usuario es quien dice ser y tiene suficientes privilegios para llevar a cabo todas las

operaciones que desee realizar. Debe ser capaz de notificar al administrador acerca de cualquier anomalía (Mojsiejczuk, 2007)

1.3.herramientas de seguridad.

Una herramienta de seguridad es un programa que corre en espacio de usuario diseñado para ayudar al administrador, alertándolo o realizando por sí mismo las acciones necesarias a mantener un sistema seguro. (Mojsiejczuk, 2007)

Lo importante es proteger la información. Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos), son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. (Mojsiejczuk, 2007)

- La confidencialidad: se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas “pinchadas”, la interceptación o recepción electromagnética no autorizada, o la simple intrusión directa en los equipos donde la información está físicamente almacenada. (Mojsiejczuk, 2007)
- La integridad: se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder

descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre. (Mojsiejczuk, 2007)

- Disponibilidad: la disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor. (Mojsiejczuk, 2007)

1.4.tipos de amenazas informáticas.

Existen diferentes tipos para poder vulnerar la seguridad informática y afectar el correcto funcionamiento o robar información de un equipo informático. (Luzardo, 2010)

Antes de iniciar a mencionar las diversas amenazas que existen se debe definir que es un virus informático.

Virus Informático.

Un virus informático en una definición sencilla y clara es un programa que se copia automáticamente y que como único objetivo que tiene es la de alterar el funcionamiento de la computadora, sin la autorización o el conocimiento del usuario. (Alegsa, Definición de Virus (informático), 2015)

También una de las características de un virus informático es el auto replicarse y ejecutarse por sí mismo, habitualmente reemplazan archivos ejecutables por otros infectados con el código de este. El código del virus puede quedar alojado en la memoria RAM aun cuando el programa que contenía el virus haya terminado de ejecutarse.

Daños.

Algunos de los principales daños que puede ocasionar un virus se encuentra el consumo de recursos de un computador, cortes en el sistema de la información o daños a nivel de datos, pérdida de información, etc.

Formas de contagio.

Una de las formas de contagio más habituales es la de ejecutar un archivo que ya se encuentre infectado por un virus, generalmente son archivos adjuntos enviados por correo electrónico o bien pueden ser archivos que el mismo usuario descarga a través de internet.

Como combatirlos.

La forma más habitual es con un antivirus, pero más que un antivirus este debe estar al día con las actualizaciones de base de datos, ya que por día se crean un aproximado de 30.000 virus, pero aun así con un buen software antivirus que se posea no es garantía de que un virus infecte a una computadora porque los creadores de virus son demasiados astutos para eso y siempre encuentra una vulnerabilidad para poder afectar los archivos. Entre algunos softwares antivirus gratuitos están Avg free, Avast, Panda Free antivirus, etc., y algunos antivirus con versión de paga Kaspersky, Bitdefender, Norton, Panda, etc.

A continuación, se enlistaron algunos virus que afectan el rendimiento de un equipo informático o podrían robar información y algunos métodos o técnicas para poder combatirlos.

Spyware

Es un código malicioso el cual su principal objetivo es recoger información sobre las actividades principales de un usuario en su computador (tendencias de navegación), para permitir el despliegue sin autorización ventanas emergentes de mercadeo o para robar información personal. (Tarazona T., 2007)

Forma de combatirlos.

En algunos casos un antivirus es incapaz de encontrar Spyware, por motivo de que no esté actualizado o por el simple hecho de que no pueda reconocer como una potencial amenaza, la mejor forma de combatirlo es instalando un anti spyware que son los más eficaces para combatir este tipo de problemas. Entre algunos anti spyware se pueden mencionar Malware bytes, SpyBot Search & Destroy, SpywareBlaster, etc. (Luzardo, 2010)

Gusanos. (Worms).

Es un tipo de virus informático el cual tiene la característica de duplicarse a sí mismo y que generalmente son invisibles al usuario. Un virus infecta y corrompe los archivos de la computadora, en cambio un gusano su objetivo es dañar la red consumiendo el ancho de banda, además de que consumen los recursos del sistema volviéndolas lentas. (Luzardo, 2010)

Formas de combatirlos.

Debido a que son considerados otro tipo de virus informático, un Antivirus actualizado es capaz de combatir esta amenaza y mantener a salvo de este virus el equipo de cómputo o la red.

Trojanos (caballos de Troya)

Es un programa malicioso capaz de alojarse en la computadora y permitir el acceso a usuarios externos, a través de una red local o de internet con el único fin de recabar información o control remotamente el equipo. (Luzardo, 2010)

Comúnmente un trojano se encuentra alojado en una aplicación que puede ser una imagen, un video, un archivo de música, etc. Habitualmente los trojanos lo utilizan para espiar en los equipos y robar las contraseñas, reiniciar o apagar la computadora sin previo aviso, controlar el equipo remotamente por otro usuario (Hackers o Lamers).

Forma de combatirlos.

Un antivirus actualizado debería eliminar la amenaza, aunque si los problemas persisten y el trojano se resiste en ser eliminado, un software anti trojano podría ser una solución para borrar este virus.

Si en el caso de que el equipo este siendo controlado remotamente lo primordial sería desconectar el equipo de la línea DSL o simplemente apagar el modem.

La última tendencia de los virus se denomina cripto-virus, el cual funciona que una vez instalada cifra o encripta toda la información contenida en el disco del equipo o en algunos casos los archivos contenidos en el disco, posteriormente se solicita una cantidad de dinero a la víctima, para que sus autores entreguen las claves para poder recuperar la información cifrada. (Tarazona T., 2007)

Phishing.

Es un ataque de ingeniería social, el objetivo principal de este ataque es obtener de manera fraudulenta datos confidenciales de un usuario, especialmente datos financieros,

aprovechando la confianza que este tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y los servicios en algunos casos con pobres medidas de seguridad. Actualmente estos ataques son bastantes sofisticados, ya que utilizan mensajes de correo electrónico y falsos sitios web. (Tarazona T., 2007)

Como combatirlo.

Con el Phishing prácticamente el error lo comete el usuario, hay que recordar que el Phishing no es más que una estafa, y esto se basa en el que los ciberdelincuentes desean obtener información personal como números de tarjetas de crédito, cuentas bancarias, etc.

La mejor forma de combatirlo es estar alerta y desconfiar de mensajes de correo electrónico de desconocidos o de organizaciones que desconoce, o de páginas web que en ningún momento se ha suscrito. (Alerta en Línea, 2011)

Evitar dar información personal o financiera por correo electrónico, el correo electrónico no es método seguro para dar esta información, las compañías que operan legítimamente evitan pedir información por correo electrónico o mensajes de texto. (Alerta en Línea, 2011)

No hacer clic a los enlaces desconocidos, ni mucho menos llamar a números de teléfono que recibimos que piden actualizar nuestra información personal. (Alerta en Línea, 2011)

Si el caso de que hay que tener que suministrar información por un sitio web, deberá estar seguro de es el sitio web oficial de la compañía u organización, un sitio web seguro siempre inicia con https://, la “s” corresponde a seguro, aunque esto también no es tan

infalible ya que algunos Phishing también falsifican estos iconos. (Alerta en Línea, 2011)

Spam

Son mensajes no solicitados, especialmente por correo electrónico, el objetivo principal del spam es difundir mensajes propagandísticos o comerciales (Tarazona T., 2007)

Como combatirlo.

Actualmente no hay método eficaz poder erradicar el spam, pero si hay técnicas y recomendaciones poder reducir el spam en los correos electrónicos. (El País, 2007)

No divulgar la dirección de correo en páginas sospechosas, existen robots que capturan direcciones correo y envían masivamente spam (generalmente ofertas, comerciales o Phishing) a las direcciones de correo. (El País, 2007)

Lo más importante es no responder a un mensaje de spam, con el simple hecho de dar clic en el enlace de “eliminar suscripción”, sabrán que esa dirección es válida y por lo tanto generara más spam. (El País, 2007)

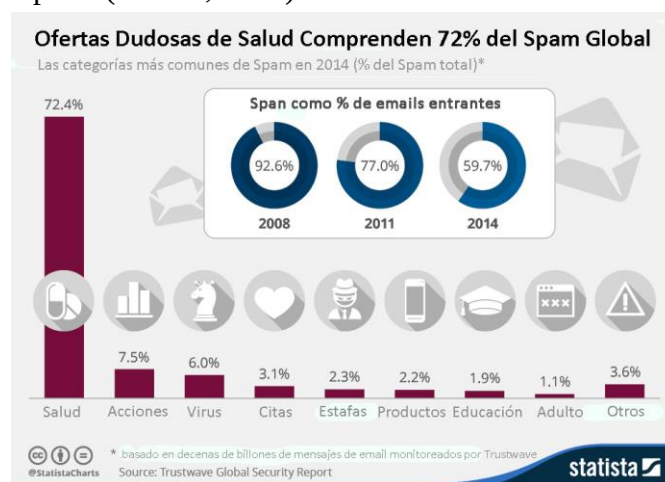


Figura 1. Gráfico de spam más común del año 2014.
<http://neorika.com/spam-mas-comun/>

Botnets (Zombis)

Son máquinas infectadas y controladas remotamente, que se comportan como zombis, quedando incorporadas a redes distribuidas de computadoras llamadas robots, los cuales envían de forma masiva mensajes de correo spam o códigos maliciosos, con el objetivo de atacar otros sistemas. (Ferri-Benedetti, 2010)

Las funciones que llegan a realizar un equipo infectado o controlado son:

- Envío de Spam
- Realización de ataques de denegación de servicio distribuido (DDoS)
- Alojamiento de archivos para sitios web: material pornográfico, pedófilo, Warez, cracks, sitios de Phishing, etc.
- Distribución e instalación de nuevo malware
- Abuso de publicidad online (Ferri-Benedetti, 2010)

Como combatirlo.

La forma de identificar que un equipo es parte una Botnet es en la carga del consumo de recursos, el usuario debe ser capaz de identificar cuando el equipo se vuelve lento en su funcionamiento o si el usuario es incapaz de realizar alguna acción o tarea en el equipo por el consumo de recursos. (Ferri-Benedetti, 2010)

La mejor forma de combatirlo es la de restringir las conexiones entrantes y salientes con un Firewall personal, la utilización de un Firewall previene, identifica y bloquea conexiones no deseadas. (Ferri-Benedetti, 2010)

Trashing.

Es un método que hace referencia buscar información en la basura (física o informática), no es una técnica relacionada directamente con los sistemas de la información, puesto que los atacantes se valen de otra forma de ingeniería social. Básicamente funciona en buscar en la basura documentos destruidos o alguna pieza de papel que contenga información relevante (información personal, claves, cuentas bancarias etc.) y posteriormente utilizarla según convenga, elaborando un perfil de la víctima para así robar su identidad o teniendo acceso a la información que se suponía era confidencial. (Tarazona T., 2007)

Como combatirlo.

Es recomendable la creación protocolos para eliminación de datos, desde el ámbito de las nuevas tecnologías, o desde los métodos convencionales (en este caso la incorporación de destructoras de papel es una buena opción o contratar un servicio externo seguro que se encargue de este aspecto).

1.5.antivirus.

Son herramientas diseñadas para detectar, bloquear y eliminar virus informáticos y otros programas maliciosos. (Panda Security, 2008)

Existen dos tipos de antivirus:

- Antivirus de escritorio: son aquellos que se instalan en el ordenador de forma local y protegen al equipo de ataques llegados a través de Internet y del correo electrónico, así como de dispositivos extraíbles. Trabajan incluso cuando el

ordenador no está conectado a Internet y deben ser actualizados para mantener su efectividad. (Panda Security, 2008)

- Antivirus en línea: son herramientas que no necesitan ser instaladas en nuestro ordenador y se accede a ellos mediante el navegador y solo es necesario disponer de conexión a Internet, además de un navegador actualizado. Son menos eficaces que los de escritorio ya que solo se cuenta con su protección si se está conectado a internet y no son tan completos como los de escritorio. (Panda Security, 2008)

¿Para qué sirve un antivirus y de qué protege?

- Vigilan todas las entradas y salidas de información a nuestro ordenador como son los dispositivos de almacenamiento y las vías de comunicación con Internet, como el correo electrónico, las páginas web o la mensajería instantánea (Panda Security, 2008)
- Protegen a un ordenador de la posible infección por virus y otros programas maliciosos, y en caso de infección proporcionan mecanismos para la limpieza del fichero o ficheros infectados, además de otras. (Panda Security, 2008)

1.6. antiespías.

¿Qué es un Antiespía?

Son herramientas que detectan y bloquean la instalación y ejecución de programas destinados a recopilar información sobre su actividad con el ordenador y sus hábitos de navegación, sin su conocimiento, con objetivos publicitarios o de robo de información. Escanean y eliminan de los sistemas, el software que espía nuestros hábitos y conexiones. (Panda Security, 2008)

¿Para qué sirve y de que protege?

- Controlan las descargas de ficheros desde Internet o desde el correo electrónico, analizando si se trata de un software espía.
- Impiden el control remoto de su equipo por personas no autorizadas mediante la instalación de estos programas en su ordenador.
- Escanean los dispositivos de almacenamiento y el software de sistema para detectar software espía (Panda Security, 2008).

¿De que protege?

- Protegen la privacidad de los usuarios contra cualquier software que espía sus contenidos y su actividad (conexiones, páginas web que visita...).
- Impiden que se pueda llevar un registro remoto de su actividad, hábitos o uso de su ordenador.
- Evitan la pérdida de productividad debido a la ralentización de los sistemas que infectan. (Panda Security, 2008)

1.7.cortafuegos.

¿Qué es un cortafuego?

Los cortafuegos o firewalls personales son programas que se encargan de controlar, permitiendo o denegando las conexiones entrantes y salientes de un ordenador. Las conexiones ocurren de forma general cuando nos encontramos conectados a Internet o una red local. (Panda Security, 2008).

Establecen una barrera entre su ordenador y la red a la que está conectado, bloqueando el tráfico, discriminando entre aplicaciones permitidas y las que no lo están. Ofrece

diferentes niveles de seguridad en función del uso y conocimientos del usuario. (Panda Security, 2008).

¿Para qué sirve y de que protege?

- Evitan ataques bloqueando accesos y conexiones no autorizadas, impidiendo que se produzcan. Complementa las defensas antivirus, anti software malicioso, etc.
- Bloquean el tráfico basándose en un esquema de aplicaciones fiables - no fiables.
- Ofrecen varios niveles de seguridad pre configurados para satisfacer las distintas necesidades de seguridad del usuario
- Proporcionan información sobre los intentos de ataque. (Panda Security, 2008).

¿De que protege?

- De los accesos no permitidos a través de la red.
- De los intentos automatizados de acceso a su equipo que producen saturación de los recursos, impidiendo el buen funcionamiento del mismo.
- Permiten controlar las conexiones salientes de la máquina evitando que el software malicioso que haya conseguido instalarse en un ordenador pueda establecer conexiones hacia el exterior. También es una forma de detectar cualquier actividad sospechosa en el ordenador. (Panda Security, 2008) .

1.8.amenazas por internet.

Los peligros por Internet son cada vez más complejos y van en aumento tal es así que los sistemas de seguridad se ven minimizados por la presencia de nuevos virus y personas con un alto conocimiento de Informática capaces de burlar cualquier sistema

de seguridad teniendo como lugar de refugio a Internet. (Instituto Nacional de Estadística e Informática (INEI), 2000)

Entrar en un lugar supuestamente “seguro”, los que lo consiguen simplemente se llenan de alegría, una diminuta minoría se queda en el lugar y altera todo lo que ve a su paso. Dentro de esta galería de personajes podemos nombrar a los sencillos internautas, los Hackers, Crackers o los Lamers entre un conjunto de intelectuales expertos en temas informáticos. (Instituto Nacional de Estadística e Informática (INEI), 2000)

A continuación, se mostrarán algunas amenazas que se podrían encontrar en internet y que podrían poner en peligro información personal, empresarial u organizacional.

Hacker.

Hacker es una persona con conocimientos de electrónica e informática, que prueba y modifica las cosas que tiene entre sus manos y se pasa largas horas pensando en ello. Existen dos tipos de Hackers, los Hackers en sí y los Hardware Hackers. El primero de ellos practica con las computadoras, el segundo con la electrónica. Al Hacker le entusiasma todo lo que rodea la tecnología, la telefonía celular, las computadoras, las tarjetas de crédito electrónicas o los Satélites. (Instituto Nacional de Estadística e Informática (INEI), 2000).

Cracker

Crackers en realidad son Hackers, pero con intenciones que van más allá de experimentar en casa, que se dedica única y exclusivamente a destruir sistemas electrónicos o informáticos. Alcanza satisfacción cuando logra destruir un sistema y esto se convierte en una obsesiva compulsión y aprovecha la oportunidad para demostrar al

mundo de sus conocimientos y que son capaces quebrantar los sistemas de seguridad. (Instituto Nacional de Estadística e Informática (INEI), 2000).

Los Gurús

Son los maestros y enseñan a los futuros Hackers. Normalmente se trata de personas adultas, porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma allí, para enseñar o sacar de cualquier duda al joven aprendiz. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallas que lo identifican como el mejor de su serie. El gurú no está activo, pero absorbe conocimientos ya que sigue practicando para conocimientos propios y solo enseña las técnicas más básicas. (Instituto Nacional de Estadística e Informática (INEI), 2000)

Los Lamers

Estos personajes son peligrosos, no tienen conocimientos y creen tener el mundo en sus manos. Si cae en sus manos un programa generador de Virus, este, lo suelta en la red sin comprender el daño que puede causar. Es el típico tipo que se pasa la vida “molestando” a los demás, enviando bombas lógicas o Virus por la Red. (Instituto Nacional de Estadística e Informática (INEI), 2000)

Los CopyHackers

Pertenecen a una nueva generación de falsificadores. Obtienen lo que les interesa y se lo venden a alguien sin escrúpulos que comercializará el sistema posteriormente. Estas personas quieren vivir del cuento y son obsesivas. Suelen leer todo lo que hay en la Red y las revistas técnicas en busca de alguna persona que sabe algo. Después se pone en

contacto con esta persona y trata de sacarle la idea. Cuando lo consigue, no tiene escrúpulos en copiarlo, llevarlo a cabo y vendérselo a otra persona denominado “bucanero”. (Instituto Nacional de Estadística e Informática (INEI), 2000)

Los bucaneros

Se trata de comerciantes, por que venden los productos comprados a los CopyHackers productos como últimos programas de aplicación crackeados. Suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero sí de negocios. El bucanero compra al CopyHacker y revende el producto bajo un nombre comercial. En realidad, es un empresario con mucha obsesión a ganar dinero rápido y de forma deshonesto. (Instituto Nacional de Estadística e Informática (INEI), 2000)

El Newbie

Que significa novato, persona que aprende lentamente, se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la página web para seguir las instrucciones de nuevo. Es el típico tipo, simple y nada peligroso. (Instituto Nacional de Estadística e Informática (INEI), 2000)

Wannaber

Toda aquella persona que quiere ser Hacker, pero su capacidad intelectual y conocimientos es insuficiente, no consigue aprender nada y se exprime al máximo. Y al final nunca logra nada, sin embargo, posee paciencia y actitud positiva. De lo contrario se sumergiría en una grave depresión. (Instituto Nacional de Estadística e Informática (INEI), 2000).

Evitar amenazas por internet.

Seguramente internet a creado un impacto en la vida diaria de las personas y compañías, y la mayoría de tareas que realizamos diariamente, siempre está presente el uso de dispositivos con conexión a internet (móviles, Tablet, GPS, etc.). para poder reducir el riesgo de algún virus en interne se pueden mencionar:

- Evitar enlaces sospechosos, uno de los casos más comunes que un usuario comete en internet, evita dar clic a hipervínculos o enlaces sospechosos sin previa revisión o recomendación, la mayoría de antivirus tiene bloqueadores automáticos que evitan que se puedan acceder a páginas web que poseen malware o virus. (InfoSpyware, 2010)
- Descargar de sitios oficiales, los programas populares muchas veces son alterados o modificados por versiones que podrían contener malware o algún otro código malicioso, por eso siempre descarga los programas de los sitios oficiales. (InfoSpyware, 2010)
- Usar softwares de protección, es recomendable siempre utilizar programas de seguridad a la hora de navegar por internet, software como antivirus, firewalls y antimalware, pueden reducir el riesgo de amenazas que se propagan por internet. (InfoSpyware, 2010)

1.9. amenazas en una red inalámbrica o wireless.

¿Qué es una Red inalámbrica? es una red que permite a las computadoras o a otros dispositivos, comunicarse entre sí a través de tecnologías de frecuencias radiofónicas

(RF por las iniciales en inglés de Radio Frequency). En simples palabras permite al usuario conectarse a internet sin la utilización de cables. (Radvan, 2010)

Clasificación de las redes.

Las redes inalámbricas se pueden clasificar de dos formas.

- Redes Privadas: son aquellas que pertenecen exclusivamente a una compañía u organización en particular, la información no está compartida con otras redes u organizaciones. En una red privada la información está protegida.
- Redes Públicas: es una red en la cual circula información de compañías u organizaciones. La red pública siempre es menos segura que una privada, es de bajo costo y no requiere que un administrador de red local de mantenimiento a estas redes. Un ejemplo de red pública es el internet. (Gonzáles Morales, 2006) (Gonzáles Morales, 2006).

Uno de los grandes problemas que poseen las redes inalámbricas es la débil seguridad que posee y más si se conecta a una red pública que es la que casi siempre carece de seguridad de autenticación.

Riesgos de seguridad.

Los puntos de conexión gratuitos o redes abiertas que generalmente no necesita de ninguna clave para conectarse son las más atractivas para los usuarios, pero también son atractivas para los ciberdelicuentes como los hackers, esta vulnerabilidad crea una oportunidad increíble para que los hackers tengan acceso ilimitado a los dispositivos sin protección. (Kaspersky, 2016)

Entre algunos de los tipos de riesgos que se podrían encontrar en red inalámbrica sin seguridad se encuentran:

- Cracking de contraseñas, los puntos de acceso de una red inalámbrica que cuentan con protocolo WEP, son fáciles de crackear las contraseñas. (NetWorkWorld, 2016)
- Hotspot falsos o redes gemelas, básicamente son SSDI ilegales, que imitan a las verdaderas con el único fin de interceptar los datos que se pudieran transmitir, los hackers son los que más imitan este tipo de amenazas. (NetWorkWorld, 2016)
- Espionaje, los usuarios que estén conectados en una red inalámbrica sin protección corren el riesgo de que sus datos sean interceptados por ciberespías. (NetWorkWorld, 2016)
- Infección de dispositivos, al estar conectado en una red WIFI ajena, usuarios malintencionados conectados a la misma red podrían infectar los equipos con virus, Malware, etc.

Protección en redes inalámbricas.

- Cambiar las claves y protocolos que vienen por defecto, comúnmente el protocolo WEP es el protocolo por defecto y las claves existen una gama de software y aplicaciones para móviles para intentar vulnerar la clave.
- Si es posible cambiar a un protocolo de seguridad como WPA o WPA2 que es el más avanzado en seguridad inalámbrica.

- Otra recomendación en redes inalámbricas es cambiar los nombres WIFI o SSID, usualmente viene con el SSID por defecto y esta algunas veces trae el nombre del operador o algunas letras de la clave por defecto.

1.10. protección informática con cifrado.

¿Qué es el Cifrado?

La criptografía (del griego oculta y escribir, literalmente escritura oculta) es el arte o ciencia de cifrar (encriptar) y descifrar (desencriptar) información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que solo puedan ser leídos por las personas a quienes van dirigidos. (Pousa, 2011)

Existen dos tipos básicos de sistemas de cifrado:

Sistemas de cifrado simétricos (o sistemas de clave secreta o de clave privada).

Los sistemas simétricos utilizan la misma clave para encriptar y desencriptar. Ejemplos DES, AES. (Pousa, 2011)

AES

Es un algoritmo de cifrado simétrico desarrollado por los estudiantes Vincent Rijmen y Joan Daemen de la Katholieke Universiteit Leuven en Bélgica, bajo el nombre "Rijndael" fue presentado en 1997 al concurso organizado por el Instituto Nacional de Normas y Tecnologías (NIST) para elegir el mejor algoritmo de cifrado; el algoritmo gano el concurso transformándose en un estándar en el año 2002, con algunos cambios fue posteriormente renombrado AES (Advanced Encryption Standard) y se convirtió en uno de los algoritmos más utilizados en la actualidad.

En 2003, el gobierno de los Estados Unidos anuncio que el algoritmo era lo suficientemente seguro y que podía ser usado para protección nacional de información. Hasta el momento no se conocen ataques eficientes, los únicos conocidos son los denominados ataques de canal auxiliar. (Pousa, 2011)

Un ataque de canal auxiliar no ataca al algoritmo de cifrado, sino que aprovecha vulnerabilidades de las implementaciones que pueden revelar datos a medida que se realiza el cifrado (Pousa, 2011)

Sistemas de cifrado asimétrico (o sistemas de clave pública).

Los sistemas asimétricos utilizan dos claves, una privada y una publica (siendo una la inversa de la otra). Ambas pueden ser usadas para encriptar y desencriptar información. (Pousa, 2011).

1.11.seguridad en sistema operativo android.

¿Qué es Android? Es un sistema operativo para dispositivos móviles como teléfonos inteligentes, tabletas, TV y otros dispositivos. Basado en el núcleo Linux, es desarrollado por la Open Handset Alliance, la cual es liderada por Google, usando diversos conjuntos de herramientas de software de código abierto para dispositivos móviles. (Molina Rivera, Sandoval Cardona, & Toledo Franco, 2012).

Tipos de amenazas en Android.

Con el aumento de la población son muchas los usuarios que hacen uso de un dispositivo móvil Smartphone o tabletas para navegar por la web, estar en las redes sociales, revisar el correo electrónico, descargar música, videos, comprar o realizar transacciones bancarias vía online, etc. Pero también es así el riesgo que corren, porque los

cibercriminales y el malware amenazan cada día con robar información personal o bancaria. (Ávila Mejía, 2011)

El porqué del aumento de malware en Android se describirán a continuación.

- El sistema operativo el Android es el más utiliza en los Smartphone con cuota de mercado aproximado del 70 %. (Kaspersky, 2016)
- Por ser una plataforma abierta, la facilidad con que se crean aplicaciones y variedad de aplicaciones no oficiales que existen el mercado son influyentes para la seguridad en Android. (Kaspersky, 2016)

¿Qué tipos amenazas afectan en Android actualmente?

Las amenazas maliciosas más comunes Android se encuentran:

- Virus troyanos por SMS.
- Módulos de privacidad.
- Exploits para tener acceso de administrador en Smartphone. (Kaspersky, 2016)

Según datos de la firma de seguridad Kaspersky, reveló que Android es el sistema operativo móvil con más virus y malware, los principales canales donde se propagan estas amenazas son las tiendas no oficiales de aplicaciones y casi la mitad (49 %) son ficheros maliciosos como troyanos que son capaces de robar datos de los teléfonos como contactos, nombres, direcciones, números de teléfono, etc. La otra parte la comprendía de malware como troyanos SMS y por ultimo estaban los Backdoors, de los cuales podían tomar control de los dispositivos. (Kaspersky, 2016)

Protección en Android.

Muchos usuarios pensarán que instalar un antivirus en Android sería la solución más acertada, sin embargo, muchos de los antivirus que existen para Android, no son muy útiles y solo se encargan de consumir muchos recursos sin aportar la suficiente seguridad que se necesita.

Uno de los consejos más comunes es mantener actualizados los dispositivos como las aplicaciones, generalmente muchas de las aplicaciones incluyen correcciones de errores.

- Siempre descargar aplicaciones de sitios legítimos o en caso de Android descargarlas de Google Play. (KasperskyLab, 2016)
- Mantener bloqueado el dispositivo, si cae en manos ajenas podrías ser víctimas del robo de información como los contactos, nombres, acceso a las aplicaciones, etc.
- Evitar descargar aplicaciones de terceros, las aplicaciones de terceros usualmente contienen código malicioso. (KasperskyLab, 2016)
- Evitar el wifi gratuito, estas conexiones no cuentan con seguridad alguna y son más propensas para el robo de información. (KasperskyLab, 2016)

1.12. disco multimedia.

Un DVD multimedia, es aquel DVD que presenta un contenido multimedia, como sonido, texto, imágenes, movimiento, video entre otros, destinado a ser visto especialmente en las PC, y en casos especiales en las computadoras Mac.

Las características principales que poseen son un Autorun, que hace que una vez insertado en la lectora de DVD, se empiece a reproducir automáticamente, generalmente a pantalla completa.

El contenido generalmente esta realizado con software especiales, uno de ellos el Director de Macromedia, con mayores alcances, y el otro con softwares dedicados como My autoplay que se usa para aplicaciones interactivas, ambos tienen capacidad de realizar lo que llamamos un proyector que hace que tras el diseño se pueda ver correctamente en las computadoras, sin necesidad de instalar ningún software adicional, esto claro si el diseño está correcto.

Un DVD multimedia se usa para mostrar lo que deseemos, como un catálogo de productos, la presentación de una empresa, un video a un cierto tamaño y tiempo entre otros, puede ser el contenido muy sencillo y llamativo, o complejo y con gran cantidad de información.

1.13.manual impreso.

El manual de usuario es un documento técnico de un determinado sistema que intenta dar asistencia a sus usuarios.

Los manuales de usuario generalmente son incluidos a dispositivos electrónicos, hardware de computadora y aplicaciones. El manual de usuario puede venir tanto en forma de libro como en forma de documento digital, e incluso poder ser consultado por internet.

En general, un manual de usuario debería poder ser entendido por cualquier usuario principiante, como así también serle útil a usuarios avanzados.

Un manual de usuario completo suele tener:

- Un prefacio, con información sobre cómo usar el propio manual.
- Un índice.

- Una guía rápida sobre cómo usar las funciones principales del sistema.
- Una sección para la resolución de problemas.
- Una FAQ.
- Información de contacto.
- Un glosario.

1.14.ley especial contra delitos informáticos y conexos.

Con el objetivo de proteger derechos fundamentales como el honor, intimidad, integridad sexual, propiedad intelectual y seguridad pública; la Asamblea Legislativa aprobó, con 70 votos, la Ley Especial contra los Delitos Informáticos y Conexos; la cual abonará a la prevención y sanción de los de los hechos punibles cometidos mediante el uso de las Tecnologías de la Información y Comunicación (TIC), que afecten la imagen de personas naturales o jurídicas. (Asamblea Legislativa República de El Salvador., 2016)

La normativa establece que se considerará comisión de Delito Informático cuando se haga uso de las TIC, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información (Asamblea Legislativa República de El Salvador., 2016)

Dicha ley será aplicable a hechos punibles cometidos total o parcialmente en territorio nacional o en lugares sometidos a su jurisdicción. También se aplicará a personas naturales o jurídicas; nacionales o extranjeras cuando se afectaren bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador. (Asamblea Legislativa República de El Salvador., 2016)

Entre los aspectos que contempla la normativa destacan se dividen por naturaleza en: Delitos contra los sistemas tecnológicos de información; delitos informáticos; delitos informáticos relacionados con el contenido de los datos; delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad y delito contra el orden económico. (Asamblea Legislativa República de El Salvador., 2016)

En relación a los delitos informáticos se regulan: la estafa, fraude y espionaje informático; así como el hurto por medios informáticos y; las técnicas de denegación de servicio. (Asamblea Legislativa República de El Salvador., 2016).

También se protegerá la integridad de las personas naturales o jurídicas, en relación a obtener información de carácter confidencial. El artículo 25 de la normativa establece “el que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años”. (Asamblea Legislativa República de El Salvador., 2016).

1.15. ley especial contra actos de terrorismo

Rama de derecho: DERECHO PENAL

Materia: SISTEMA JUDICIAL

Sub-Materia: PENAL Y PROCEDIMIENTOS

Título: LEY ESPECIAL CONTRA ACTOS DE TERRORISMO

Tipo de Documento: LEY

Decreto No.: 108

DELITO INFORMATICO

Art. 12.- Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley: (Asamblea Legislativa de República El Salvador, 2014).

a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación Informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, Información, documentos electrónicos, soportes informáticos, programas o sistemas de Información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia de seguridad nacional, de entidades nacionales, internacionales o de otro país; (Asamblea Legislativa de República El Salvador, 2014)

b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a), de este artículo. (Asamblea Legislativa de República El Salvador, 2014)

2. Marco teórico de la solución.

2.1. kit de seguridad informática.

2.1.1 Ficha técnica de softwares de seguridad informática.

Tabla 1, *Ficha técnica de Adblock Plus.*

Ficha técnica Adblock Plus.	
Título del programa.	Adblock Plus.
Autor.	Creado por Wladimir Palant en 2006.
Temática.	Seguridad de internet.
Breve descripción.	Bloqueador de publicidad para navegadores de internet el cual está disponible para la mayoría de navegadores más conocidos, bloquea dominios conocidos que propagan
Requisitos técnicos	Sistema Operativo: Microsoft Windows 7 o superior, Linux y MAC OS. 1GB de RAM DUAL CORE 1.7 GHZ o superior. Peso: 500 KB, (puede variar en otro navegador).
Características.	-Bloquea todo tipo de anuncios publicitarios al navegar. -Desactiva el seguimiento y el historial realizado por cierta web para ofrecer publicidad personalizada. -Bloquea el acceso a determinadas páginas potencialmente peligrosas. -puede leer y crear filtros de archivos hosts.
Es compatible con la mayoría de navegadores de internet que hay el mercado Nota: Los requisitos de hardware pueden variar depende del navegador instalado.	

Tabla 2, *Ficha técnica Bestcrypt Container Encryption.*

Ficha técnica Bestcrypt Container Encryption.	
Título del programa.	BestCrypt Container Encryption
Autor.	Jetico Inc. Oy.
Temática.	Seguridad Informática.
Breve descripción.	Tipo de software que se utiliza para la encriptación de datos y carpetas en contenedores cifrados para la protección de los datos que pueda ser confidencial o importante para el usuario.
Requisitos técnicos.	Sistema operativo: Windows, Linux y MAC OS. 2GB de RAM. DUAL CORE 1.7 GHZ o superior. Peso: 19.8 Mb.

Características.	-Selecciona almacena archivos carpetas en contenedores cifrados. -Mover archivos contenedores Bestcrypt entre cualquier medio de almacenamiento, a través de Windows, Linux, y MAC OS. -Versión para Windows incluye BC wipe normal. -Cifra archivos de sistema operativo de Windows. -Encriptación de archivos y carpetas. -Protección archivos al subir a internet. -Protege la vulnerabilidad de archivos. -Crea y administra varios contenedores. -Monte unidad de cifrado como una subcarpeta. -Definir uso en entorno multiusuario. -Crear y acceso a contenedores al instante. -Trabajar con contenedores dinámicos. -Mejora la seguridad. -Contenedores mejorados ocultos.
Es utilizado para proteger archivos y carpetas con contraseña al subirlo a la nube es más seguro.	

Tabla 3, *Ficha técnica de Hotspot Shield.*

Ficha técnica de Hotspot Shield.	
Título del programa.	Hotspot Shield.
Autor.	AnchorFree Inc.
Temática.	Seguridad de internet.
Breve descripción.	Aplicación para navegador de internet el cual envía datos cifrados en redes que carecen de alguna o poca seguridad, también cuenta con la característica que puede desbloquear contenido de páginas como YouTube, Facebook, etc. Que no están permitidas en algunos países.
Requisitos técnicos.	Windows, Androide, Linux y MAC OS. 2GB de RAM. DUAL CORE 1.7 GHZ o superior. Peso: 12.8 Mb.
Características.	-Desbloqueo sitio web como YouTube, Facebook, entre otros ya sea en un centro educativo, en bibliotecas u oficina. -Navegue de forma anónima, crea un túnel cifrado entre su equipo y servidores de Hotspot Shield para permitirle realizar una actividad en línea de forma anónima. -Oculta dirección IP
Navega más seguro anónimamente desbloqueo contenido bloqueado en algunos países.	

Tabla 4, *Ficha técnica FREE VPN PROXY.*

Ficha técnica FREE VPN PROXY.	
Título del programa.	FREE VPN PROXY
Autor.	Betternet Technologies Inc.
Temática.	Seguridad para dispositivos Android.
Breve descripción.	VPN para dispositivos móviles o Tablet con sistema operativo Android ofrece una protección para cuando se conecta redes inalámbricas sin alguna seguridad. Evita cualquier censura o restricción que haya en tu país.
Requisitos técnicos.	Android versión 4.0 o superior Peso: 26.3 Mb.
Características.	-Gratis para siempre. -No requiere registro de inicio de sesión. -No se guardan las sesiones de ningún usuario. -Se conecta con un toque. -Conexión rápida, al servidor. -Desbloquea web y aplicaciones. -Navegación anónima. -Protege privacidad y asegura tu dispositivo.
Permite navegar anónimamente logrando navegar más seguro, desbloquea sitios web bloqueados o con restricción para ciertos países podemos cambiar la VPN y lograr conectarnos con los diferentes países que se encuentran en la lista de la aplicación	

Tabla 5, *Ficha técnica ANDROID DEVICE MANAGER*

Ficha técnica ANDROID DEVICE MANAGER.	
Título del programa.	Android Device Manager.
Autor.	Google Inc.
Temática.	Seguridad en dispositivos Android.
Breve descripción.	Esta aplicación con sistema operativo Android localiza en un mapa los dispositivos previamente configurados con una cuenta activa de Google. Cuenta ofrece características para poder localizar los dispositivos extraviados o robados como por ejemplo hacer sonar un móvil o Tablet a volumen alto o en caso extremo borrar los datos del dispositivo asociado, se necesita tener acceso a wifi o red de datos para realizar estas funciones.
Requisitos técnicos.	Android versión 4.0 o superior. Peso: 1.94 Mb
Características.	-Geo localiza un mapa. -Borrado de datos remoto. -Funciona con todos tus dispositivos asociados -Útil en caso de robo o pérdida. -protege información privada y datos.

Aplicación utilizada para rastrear el móvil remota mente, utilizando una pc e internet ingresando a la página oficial de Android Device Manager, es útil activa una alarma y podemos borrar los datos remotamente.

Tabla 6, *Ficha técnica CERRADURA (APP LOCK) ANDROID*

Ficha técnica CERRADURA (APP LOCK) ANDROID.	
Título del programa.	Cerradura (App Lock) Android.
Autor.	DoMobile Ltd
Temática.	Seguridad dispositivos Android.
Requisitos técnicos.	Android 4.0 o superior. Peso: 3.29 MB
Características.	-Protege cualquier aplicación usando contraseña o patrón. -Bóveda de fotos. - Bóveda de videos. -Personaliza fondos. -Bloqueo automático
Aplicación utilizada para crear patrón o contraseña el usuario elige protege el móvil su privacidad y aplicaciones importantes.	

Tabla 7, *Ficha técnica AVG ANTIVIRUS FREE*

Ficha técnica AVG ANTIVIRUS FREE.	
Título del programa.	Avg Antivirus Free.
Autor.	AVG Technologies CZ, s.r.o.
Temática.	Seguridad Informática.
Breve descripción.	Antivirus que ofrece distintas herramientas para la protección de la computadora, muy utilizado por su bajo consumo y excelente velocidad en el análisis. Versión free muy completa porque cuenta con detección de malware muy avanzada, protege contra troyanos, gusanos, spyware y rootkits.
Requisitos técnicos.	Sistema operativo: Windows 7 o superior, MAC OS y Android. 2GB de RAM. DUAL CORE 1.7 GHZ o superior. Peso: 2.80 Mb (instalador)
Características.	-Bloquea virus, spyware y otros malware. -Cubre todos los dispositivos desde un sencillo panel. -Bloquea a los hackers para poder realizar compras y operaciones bancarias con más seguridad. -Analiza vínculos de web.

	-Provee actualizaciones de seguridad a tiempo real. -Mejora la detección de malware.
Este programa es útil para prevenir virus que se encuentran en el internet o por dispositivos extraíbles como USB, Móviles, tarjetas SD entre otras.	

Tabla 8, *Ficha técnica MALWAREBYTES*

Ficha técnica MALWAREBYTES.	
Título del programa.	Malwarebytes.
Autor.	Malwarebytes
Temática.	Seguridad Informática
Breve descripción.	Software que detecta y elimina aparte de Malware, gusanos, troyanos, bots, etc. Software líder en la detección de malware y compatible con la mayoría de los principales antivirus.
Requisitos técnicos.	Sistema operativo: XP, Vista, 7, 8 y 10 2GB de RAM. DUAL CORE 1.7 GHZ o superior. Peso: 21.7 Mb
Características.	-Fácil de respirar. Búsqueda automática funciona para usted, para que nunca tenga que preocuparse de contraer la infección. Ordenador y sus datos se mantiene seguro. -Detecta y elimina malwares en su versión gratuita. -Protege frente a posibles infecciones (versión de pago) -Soporte para Windows XP, Vista, 7, 8 y 10 (32-bit y 64-bit). -Malwarebytes Anti-Rootkit integrado en el escáner -Tecnología de exploración y detección heurística avanzada. -100% compatible con los principales antivirus.
Programa utilizado para la prevención de malware virus potenciales que algún antivirus no detecta, MalwareBytes lo podrá limpiar.	

Tabla 9, *Ficha técnica COMODO FIREWALL.*

Ficha técnica COMODO FIREWALL.	
Título del programa.	COMODO FIREWALL.
Autor.	Comodo Group, Inc.
Temática.	Seguridad de internet.
Breve descripción.	Firewall personal que protege contra ataques de hackers o cualquier otro tipo

	de software malintencionado, controla aplicaciones que puedan tener acceso a internet y controlar las conexiones no autorizadas hacia y desde internet.
Requisitos técnicos.	Windows vista, 7, 8,8.1 y 10. 2GB de RAM. DUAL CORE 1.7 GHZ o superior. Peso: 217 Mb.
Características.	-Completa protección contra troyanos, root kits, spyware y hackers. -Utilidad malware Scan, que comprueba el sistema en busca de virus antes de instalar el programa. -Dos modos de instalación, uno básico con una configuración mínima, y otra avanzada donde se puede configurar muchas opciones para personas con más experiencia. -Un pequeño bloqueador de ventanas pop up. -Tiene una interfaz de programa amigable, y contiene asistentes que facilitan el proceso de configuración.
Programa utilizado para protección de virus mal intencionados en internet, bloquea las conexiones entrantes y salientes no autorizadas por software malicioso y mantiene controlada las conexiones en internet.	

2.1.2 Manual de seguridad informática.

El siguiente manual del usuario se desarrolla con el objetivo de dar apoyo como instalar y hacer uso de los programas que se estarán anexos en el DVD multimedia el cual se detalla paso a paso con capturas de imágenes el cual están incluidas en el kit software de seguridad, los programas que se integran en este kit son:

Adblock plus.

Bestcript container encryption.

Hotspot shield.

Free vpn proxy.

Android device manager.

Cerradura (app lock).

Avg antivirus.

Malwarebytes.

Comodo firewall.

El manual cuenta con la información teórica y técnica necesaria para el uso del kit de seguridad informática, enfocado a la protección de los equipos.

2.1.3 manual de instalación y uso de cerradura (applock), para dispositivos Android.

Nota: Este programa se instala en dispositivos Android versión 4.0 o superior. En estas capturas de imágenes se utilizó un emulador de aplicaciones Android para realizar los pasos para instalar la aplicación AppLock, los pasos a seguir son iguales a un dispositivo Android. El programa se puede descargar del sitio oficial en Google Play o del kit de

seguridad informática multimedia y se pasa la APK al dispositivo Android por medio del cable USB.

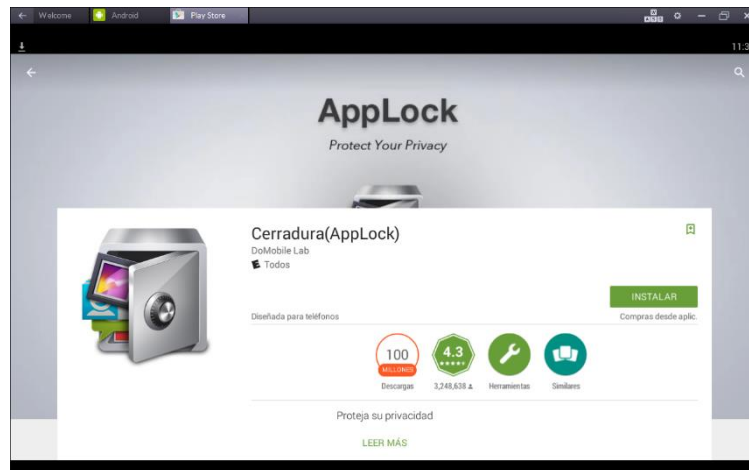


Figura 1. Instalación AppLock.

1. Instalar la aplicación ya sea del Google Play o del Kit de seguridad informática. Hacer la transferencia de la APK, al dispositivo móvil a través del pc utilizando el cable USB ver figura 1.

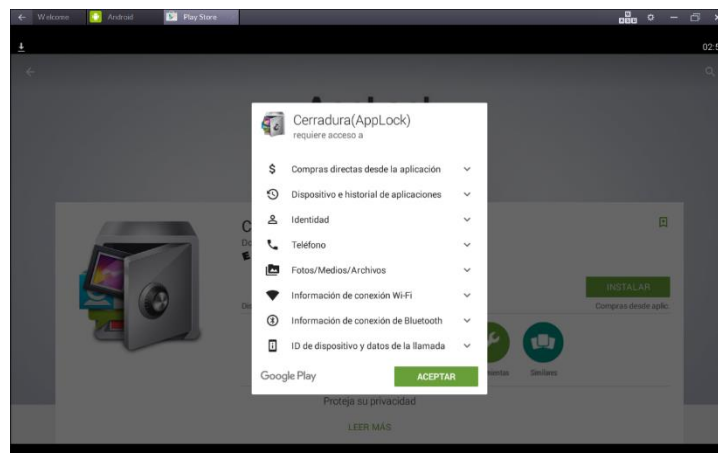


Figura 2. Instalación AppLock.



Figura 3. Instalación AppLock.

2. Clic en instalar, aceptar los términos requeridos. Ver figura 2 y se procederá a la descarga, ver figura 3 esperar hasta que se instale.

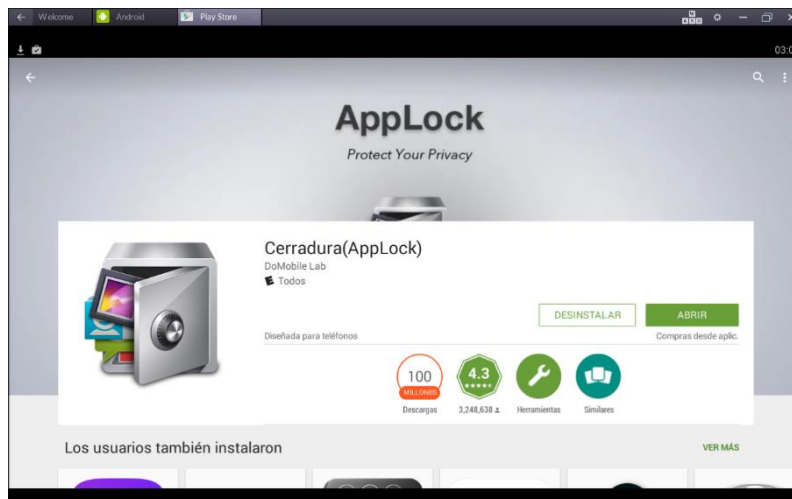


Figura 4. Instalación AppLock.

3. Se instaló correctamente la aplicación. Ver figura 4 lista para usar.

Uso de aplicación cerradura (AppLock).

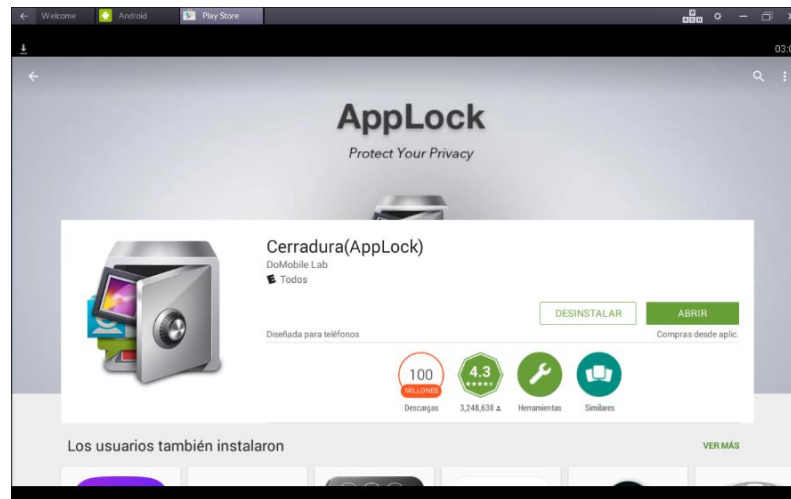


Figura 1. Instalación AppLock.

1. Clic en abrir, ver figura 1.

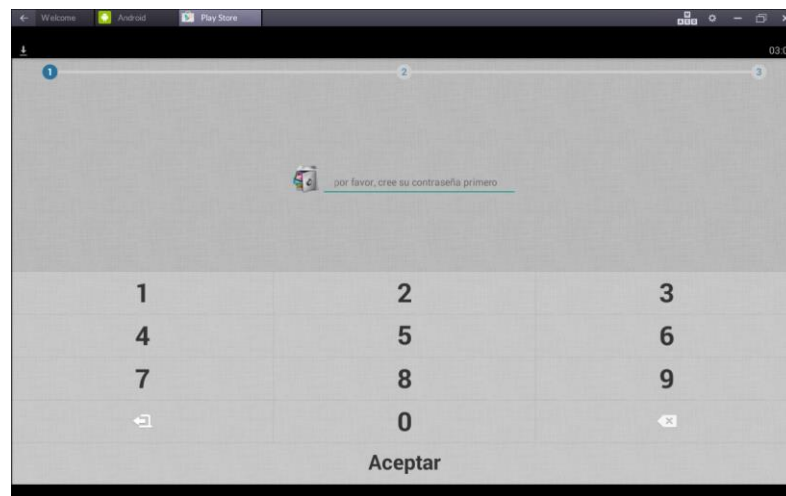


Figura 2. Crear clave.

2. Se abre el cuadro, Crear una clave que no olviden donde indica la línea celeste. Ver figura 2.

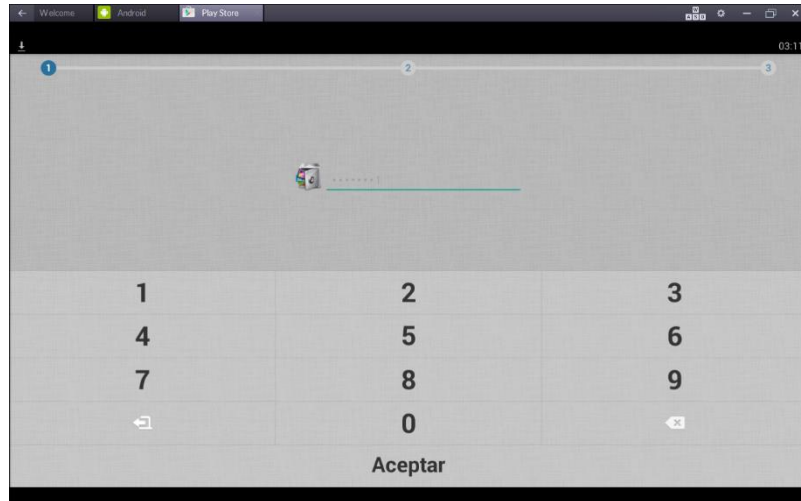


Figura 3. Ingresar clave.

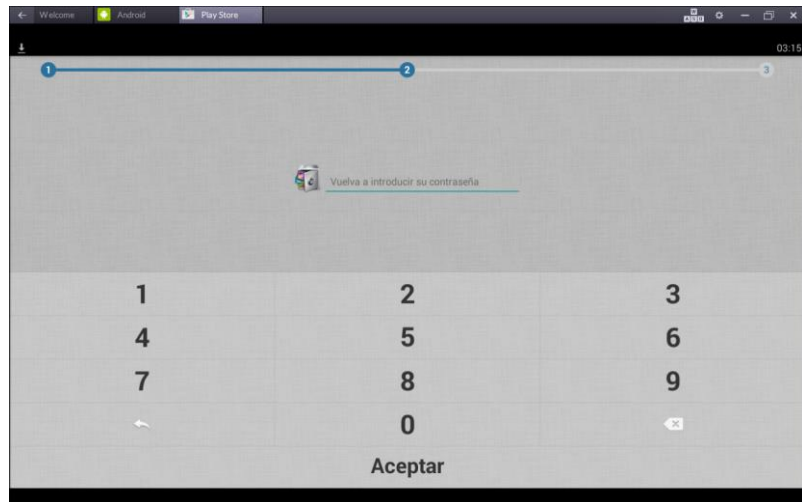


Figura 4. Ingresar clave.

3. Una vez colocada, se pide comprobación de contraseña introducir nuevamente. Ver figura 3 y 4.

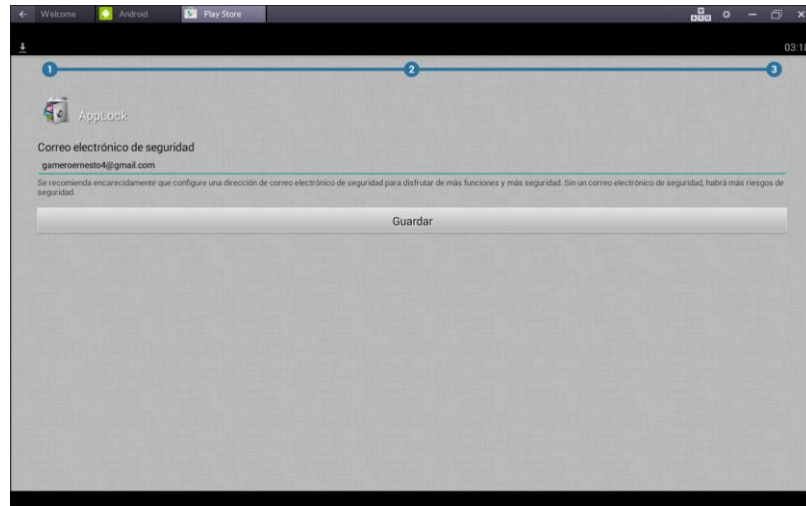


Figura 5. Ingresar correo.

4. Ya comprobado, se requiere correo electrónico asociado al dispositivo para mayor seguridad ver figura 5. Clic en guardar.

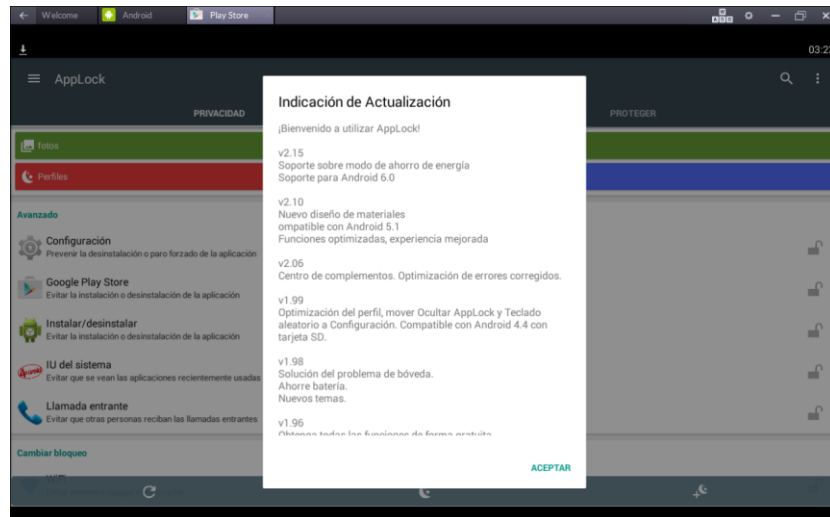


Figura 6. Indicación de actualización.

5. Habiendo guardado la contraseña, aparece el siguiente mensaje. Ver figura 6 y clic en aceptar.

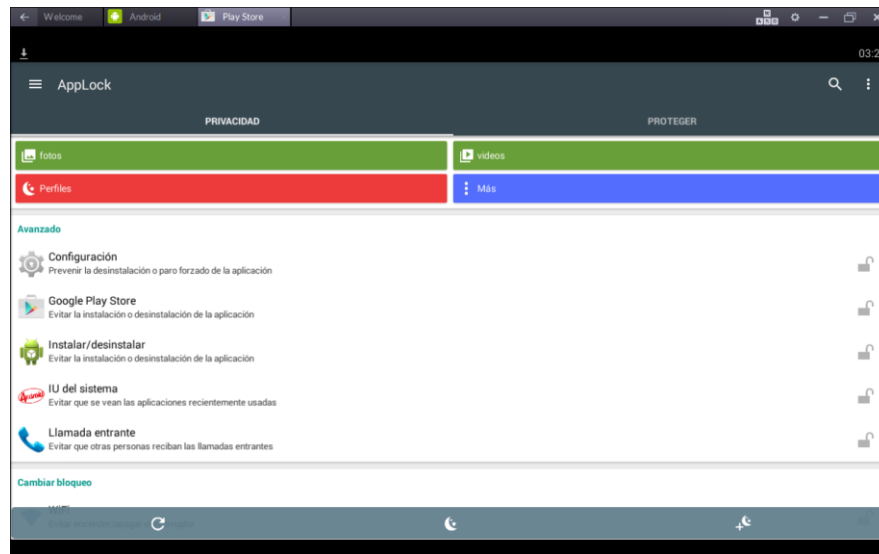


Figura 7. Lista de aplicaciones.

6. Una vez aceptado el mensaje, aparecen estas opciones Google Play, configuraciones entre otras. Son todas las aplicaciones instaladas, en el dispositivo Android, donde podemos bloquear las que se quiera proteger con cerradura, para más privacidad ver figura 7.

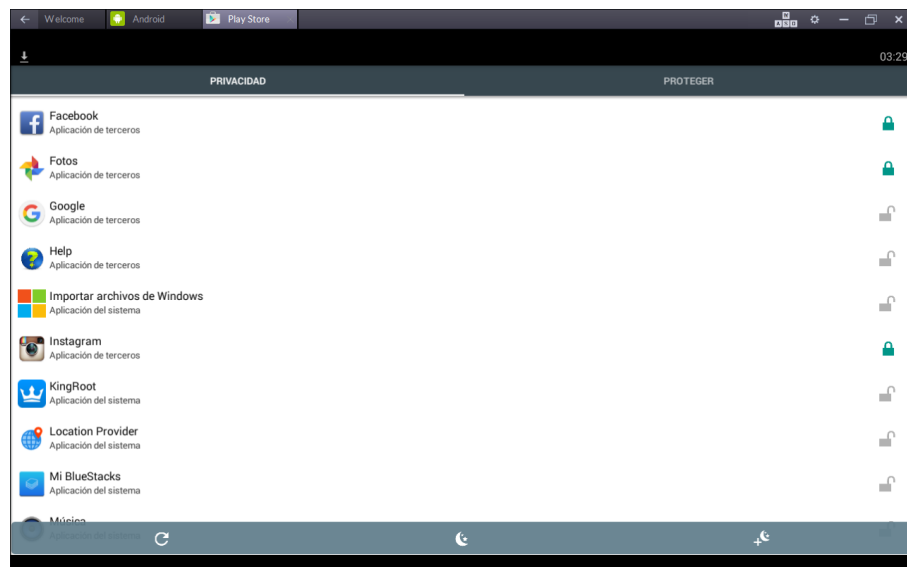


Figura 8. Lista de aplicaciones.

7. Bloquear algunas aplicaciones, ejemplo: Facebook que es lo que sucede cuando se bloquea. Volver a inicio del dispositivo Android, ver figura 8.

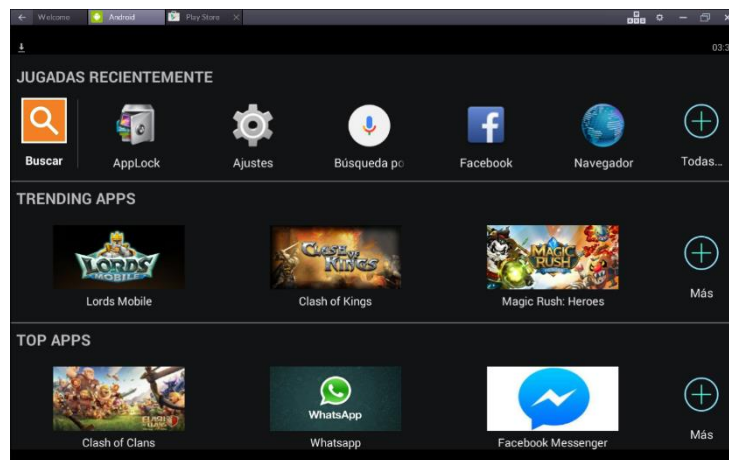


Figura 9. Menú inicio de Android.

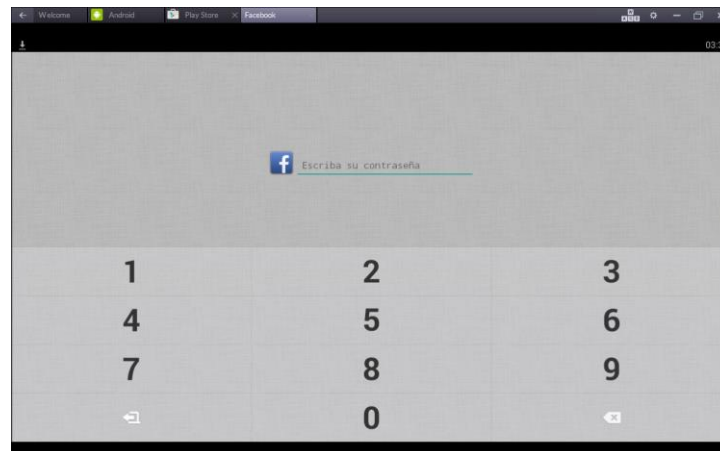


Figura 10. Página de Inicio de sesión de Facebook.

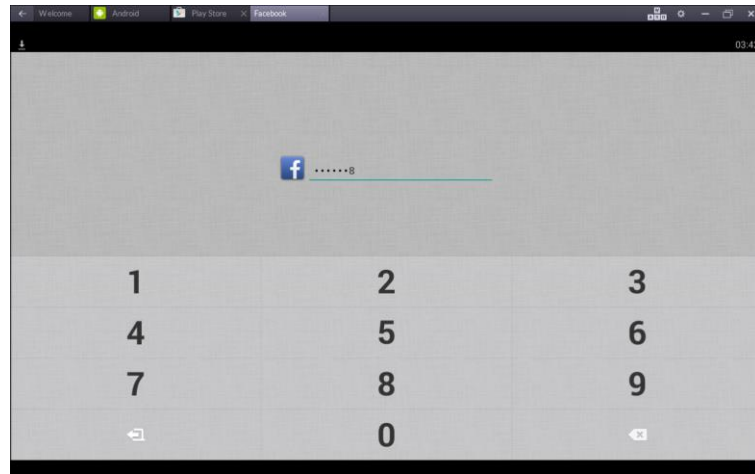


Figura 11. Página de Inicio de sesión de Facebook.

8. En inicio, abrir la aplicación Facebook, ver figura 9, 10,11. En efecto pide la clave anterior mente colocada, en el proceso 2 del uso de la aplicación cerradura (AppLock) ingresar la clave.

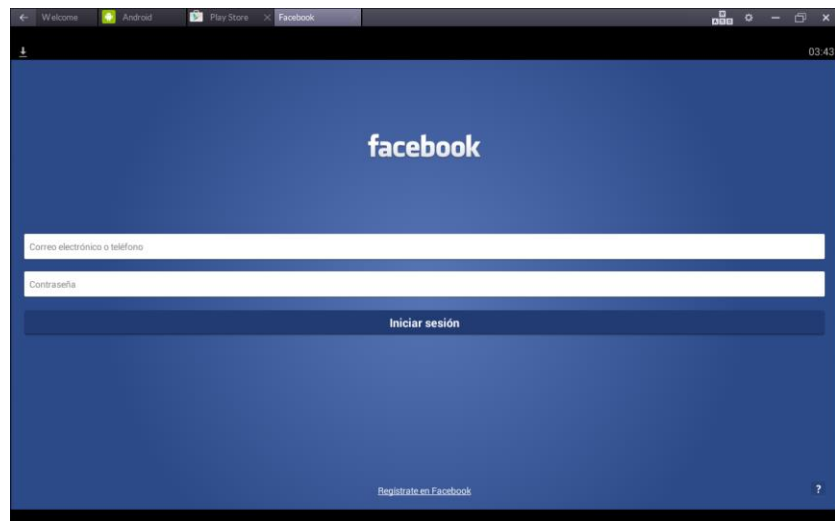


Figura 12. Página de Inicio de sesión de Facebook.

9. Ya ingresada la clave, dará acceso al Facebook. Para proceder a utilizarla. En esta ocasión no está iniciada sesión, pero si estuviera iniciada sesión aparecería la página de perfil del Facebook.

2.1.4 manual de instalación y uso adlock plus.

Nota: Este programa, es una extensión que está disponible para la mayoría de navegadores google, Firefox, opera entre otros. En el kit de seguridad informática se dejara el link del sitio donde podremos instalar el complemento Adlock plus.



Figura 1. Página oficial Adblock plus.

1. Ingresar al sitio oficial, Adblock plus, e instalar el que convenga dependiendo del navegador, en este caso, clic instalar en chrome.

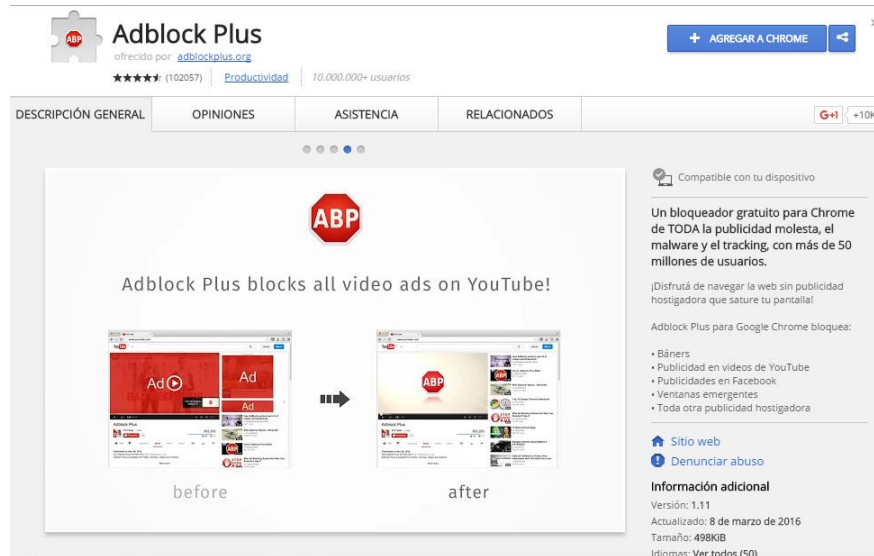


Figura 2. Página oficial Adblock plus.

2. Aparece este otro cuadro, ver figura 2. Clic en agregar a Chrome en este caso.

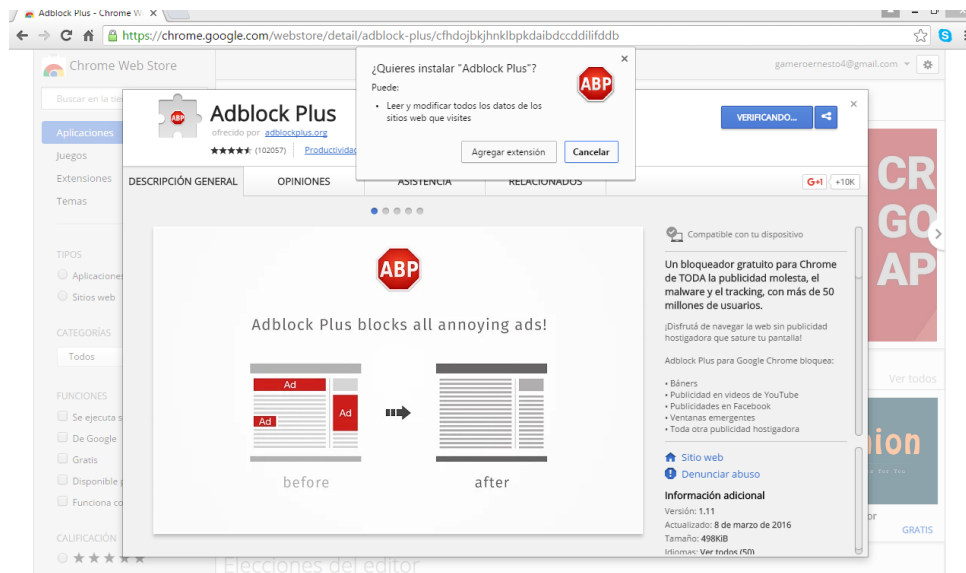


Figura 3. Página oficial Adblock plus.

3. Aparece este otro cuadro, ver figura 3. Clic en agregar extensión.

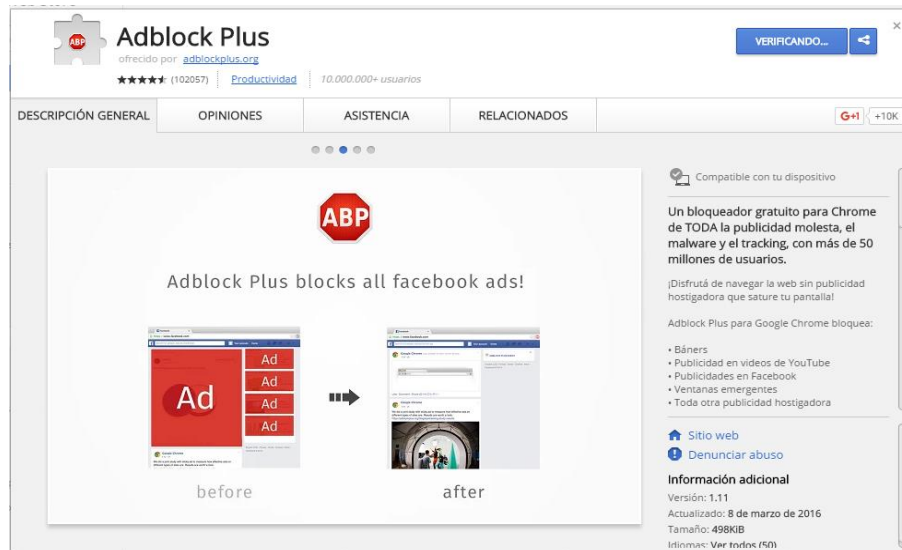


Figura 4. Página oficial Adblock plus.

4. Esperar un momento, hasta que se instale.

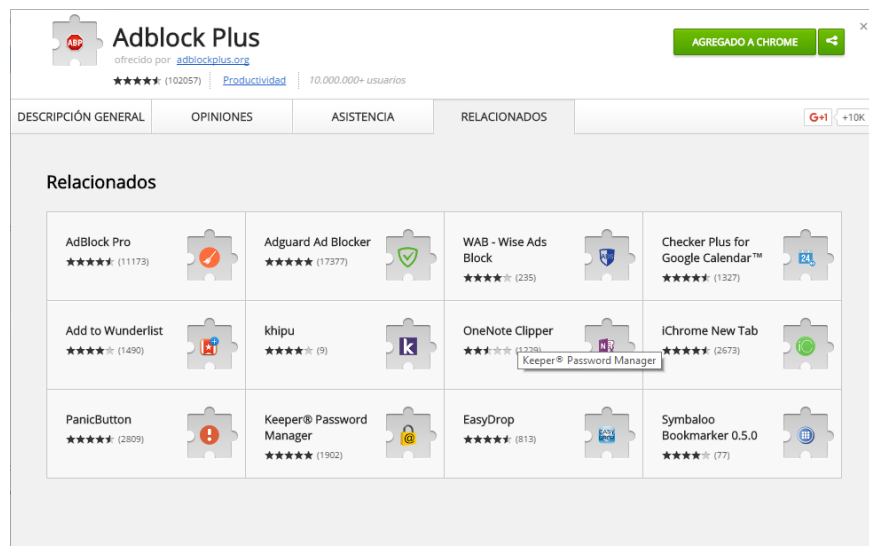


Figura 5. Página oficial Adblock plus.

5. Saldrá este cuadro, ver figura 5. En donde confirma, que se agregó el complemento.

Uso de Adblock Plus.

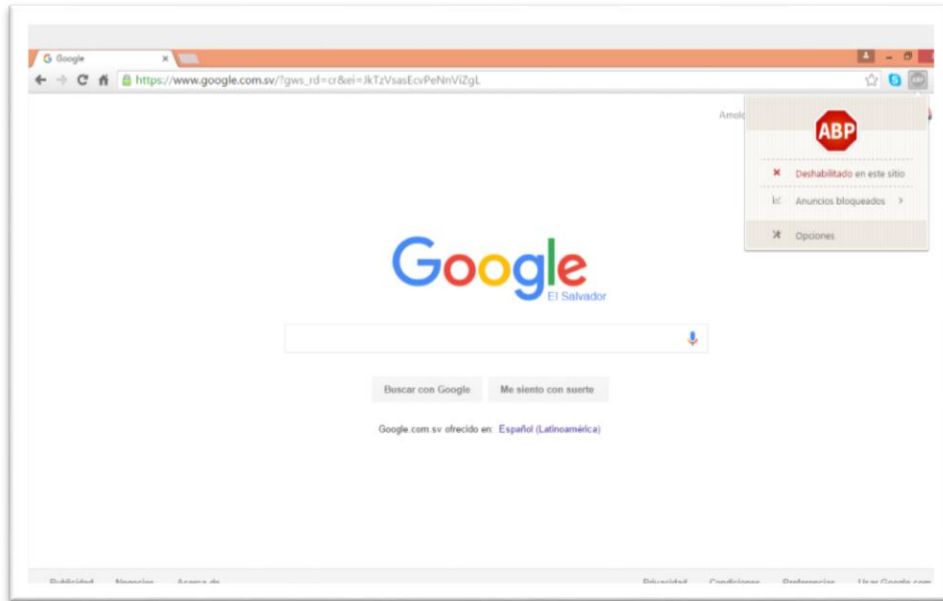


Figura 1. Adblock plus.

1. abrir google, desplegamos Adblock plus. (ABP) asegurar de activar sus opciones principales, y este en verde no en rojo ver figura 1.

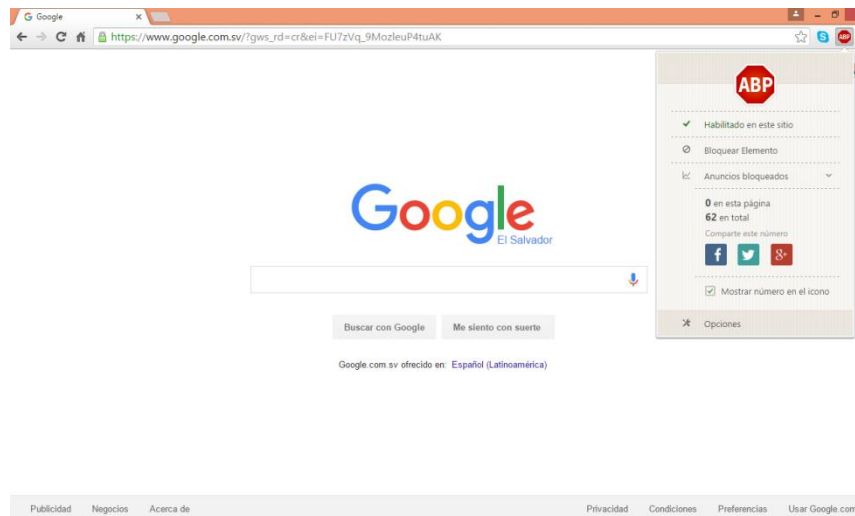


Figura 2. Adblock plus.

2. Ya habilitado, ver figura 2. El icono está en rojo, y la opción habilitado en verde.

Habilitamos la siguiente opción, anuncios bloqueados para ver la cantidad de anuncios bloqueados, la aplicación queda lista para bloquear anuncios en páginas, o en YouTube publicidad no deseada.

2.1.5.manual de instalación y uso android device manager.

Nota: para instalar esta aplicación, se necesita Android versión 4.0 o superior. En este caso se utilizó un emulador de Android para instalar la aplicación, sus pasos son los mismos para instalar en un dispositivo con sistema Android.

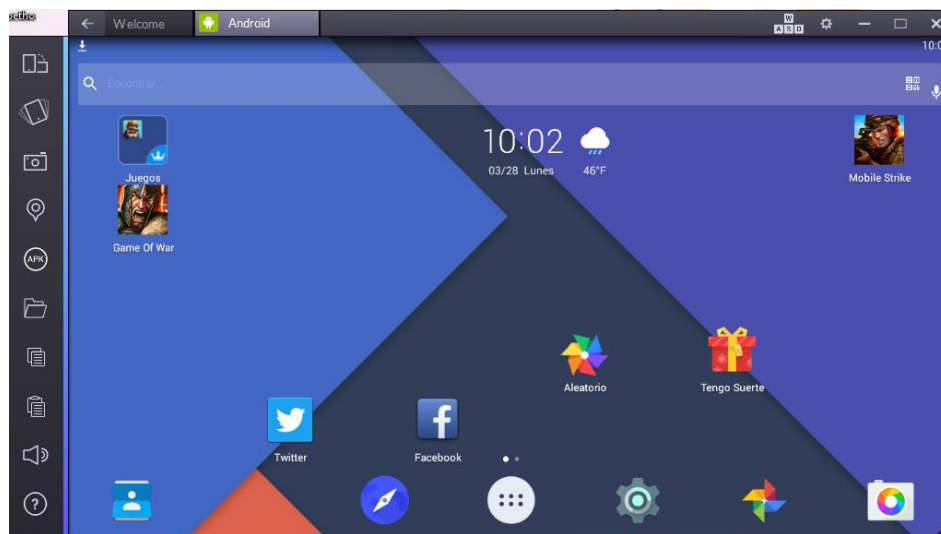


Figura 1. Menú inicio Android.

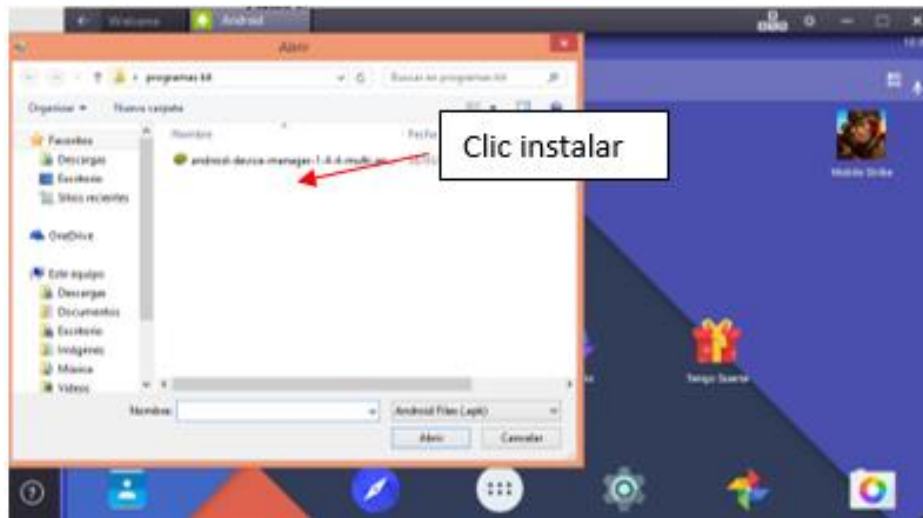


Figura 2. APK Android Device manager.

1. Buscar la APK, en el dispositivo móvil, si se trasfiere del kit de seguridad informática, o buscar en Google Play. Instalar ver figura 1 y 2.

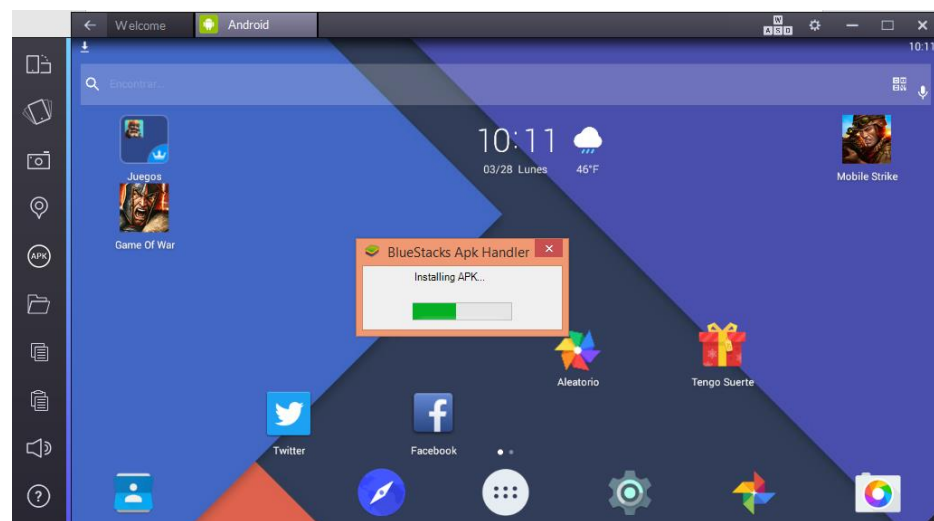


Figura 3. Aplicación Instalando.



Figura 4. Aplicación Instalada.

2. Se instalará, ver figura 3. Posterior mente buscarla en el dispositivo móvil, está lista para utilizarse ver figura 4.

Uso de Android Device Manager.

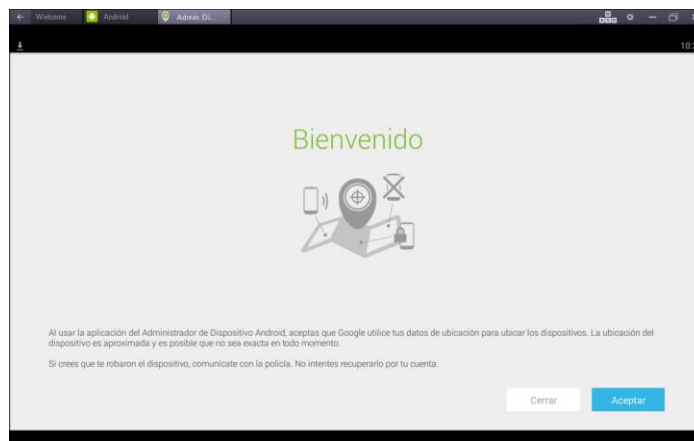


Figura 1. Instalador de Android Device Manager.

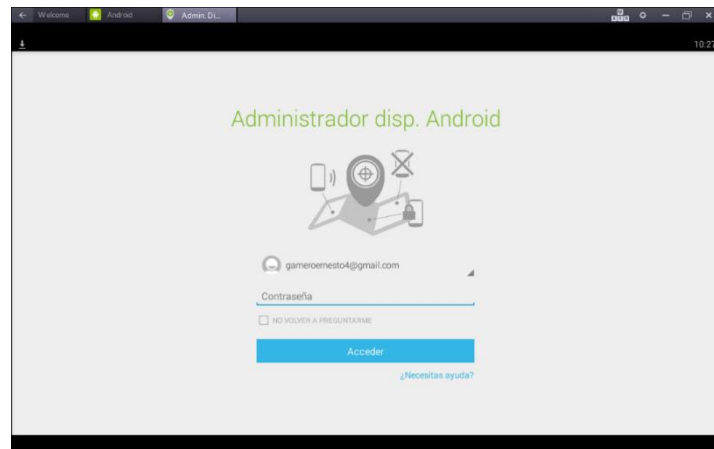


Figura 2. Administrador de dispositivos Android.

1. Abrir la aplicación, ver figura 1. Aparece el siguiente cuadro clic en aceptar, luego aparecerá otro cuadro ver figura 2, tenemos que configurar una cuenta de Gmail, con la que este asociado al Google Play, o puede ser otra, para configurar la aplicación con el dispositivo móvil.



Figura 3. Administrador de dispositivos Android.

2. Luego, aparece el siguiente menú ya configurado. Ahora ya podemos rastrear el móvil, utilizando una computadora ver figura 3.

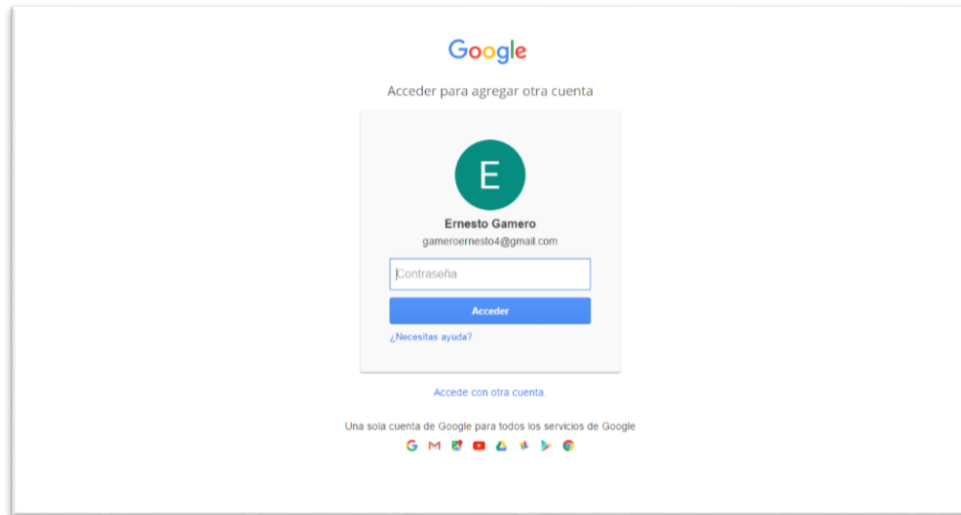


Figura 5. página oficial Android Device Manager.

3. Entrar a la página oficial, Android Device Manager. Ver figura 5, ingresar el mismo correo con el que asociamos el móvil.

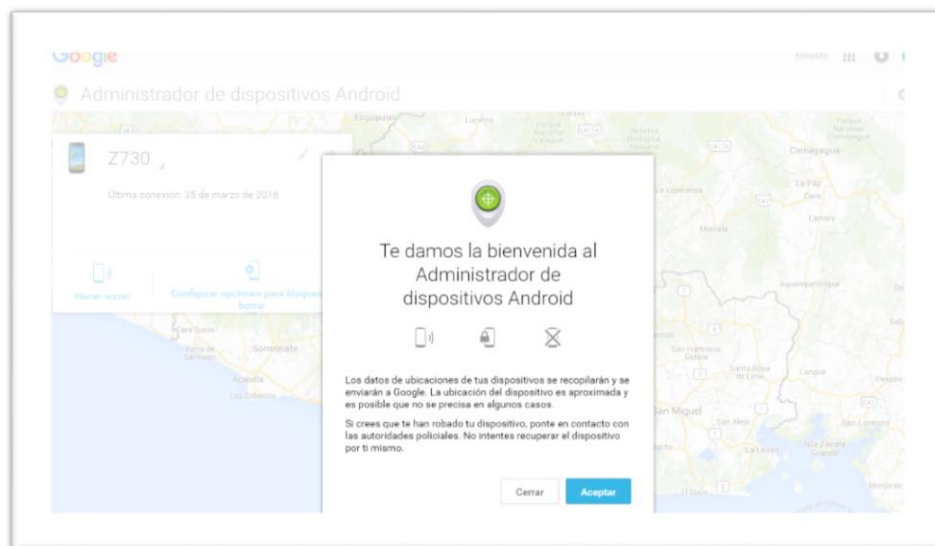


Figura 6. Android Device Manager.

4. Aparece el siguiente mensaje, aceptar ver figura 6.

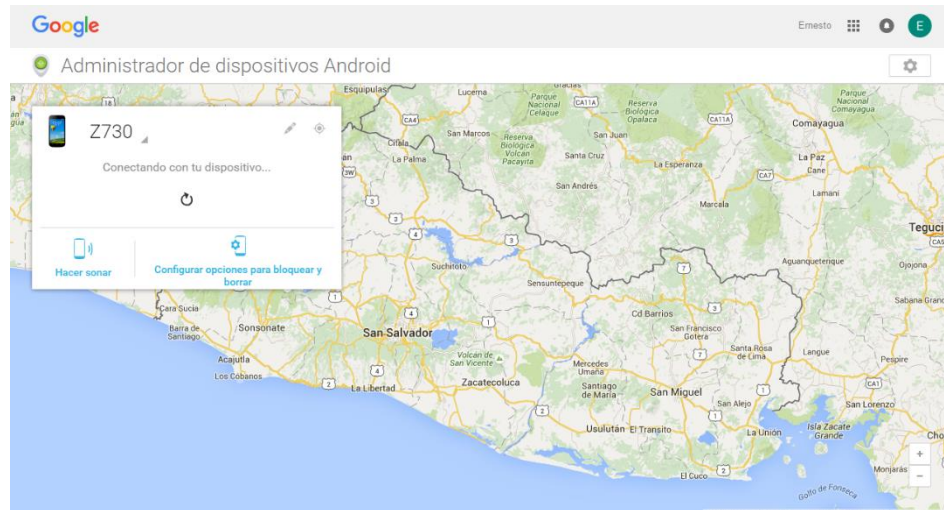


Figura 7. Administrador de dispositivos Android.

5. Aparece el administrador, donde se encuentra dos opciones, la primera hacer sonar.

Su función es: el de activar el sonido del móvil al máximo para poder localizarlo, la segunda configurar opciones para bloquear y borra. Su función es si estamos seguros de un robo, podemos borrar todos los datos del móvil, mientras este encendido, o cuando se encienda nueva mente.

2.1.6 manual de instalación y uso de hotspot shield.

Nota: En este software, se utiliza la versión elite, pero para ello se requiere un parche. Esto es para fines educativos, para tener todas las funciones disponibles, y poder desarrollar el siguiente manual.

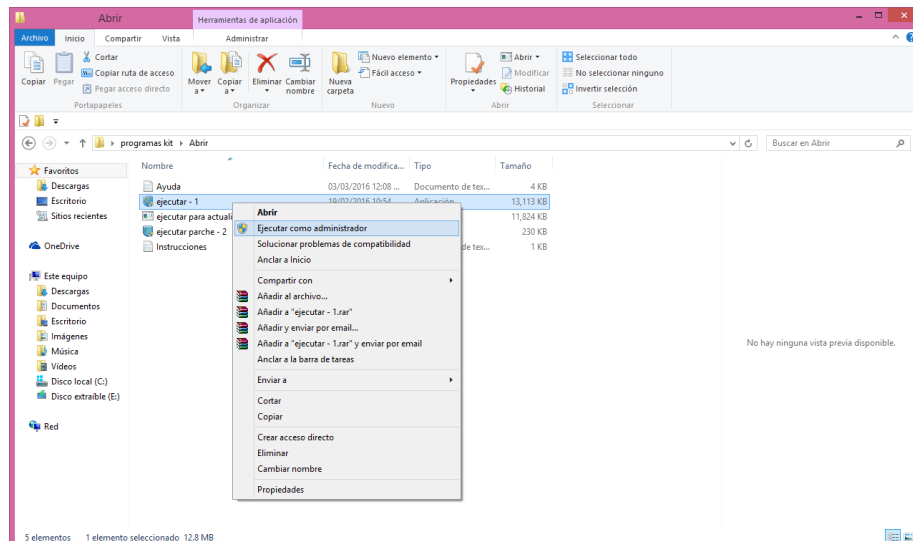


Figura 1. Instalador hotspot shield.

1. Ejecutar el software, con permisos de administrador, desactivar antivirus para evitar que lo reconozca como virus el parche ver figura 1.

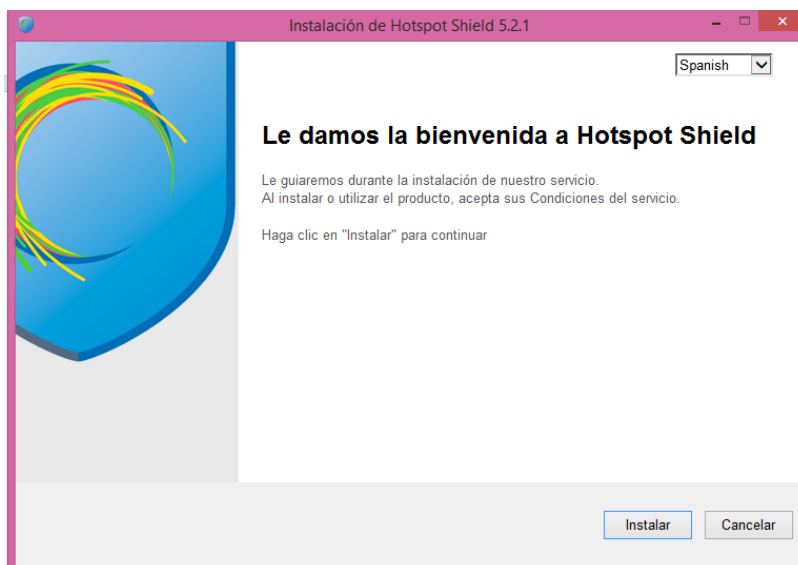


Figura 2. Instalador hotspot shield.

2. Instalar la versión 5.3.1, pero luego actualizar a la Elite, elegimos el idioma en este caso español, clic en instalar.

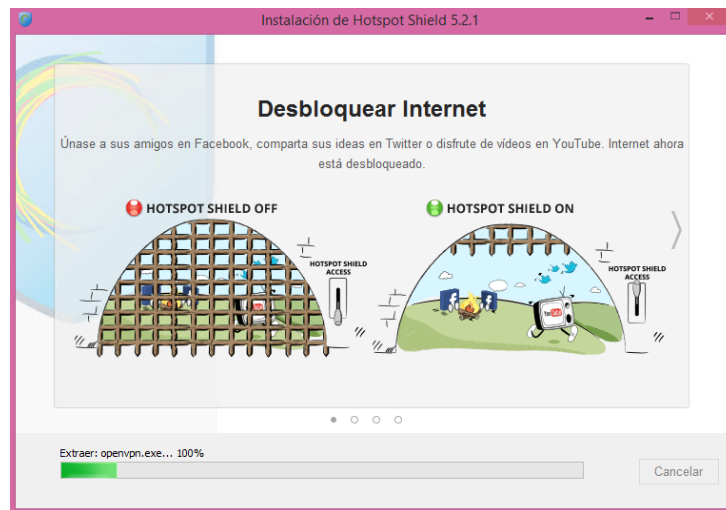


Figura 3. Instalador hotspot shield.



Figura 4. Instalador hotspot shield.



Figura 5. Instalador hotspot shield.

3. Empezará la instalación del software, ver figura 3 y 4. Una vez terminada la instalación, aparece el siguiente cuadro, ver figura 5, y terminamos de instalar haciendo clic en Terminar.



Figura 6. Menú hotspot shield.



Figura 7. Menú hotspot shield.

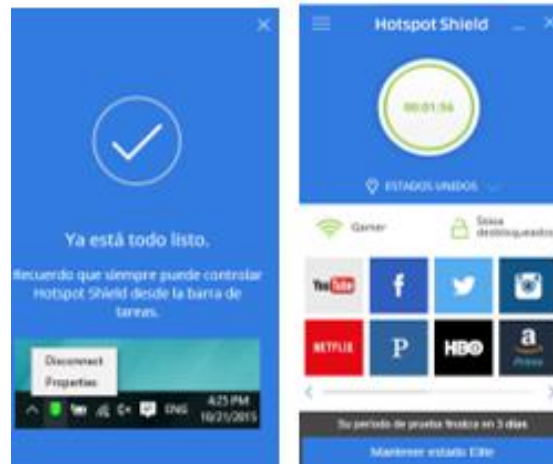


Figura 6. Menú hotspot shield. Figura 7. Menú hotspot shield.

4. Una vez terminado, saldrán estos cuadros, ver figura 6 y 7, y dar clic en entendido, hasta que sale el cuadro, ver figura 8. Ya está listo, solo hacer clic en la rueda, y listo ver figura 10.
5. Proceder a parchar solo para fines educativos.

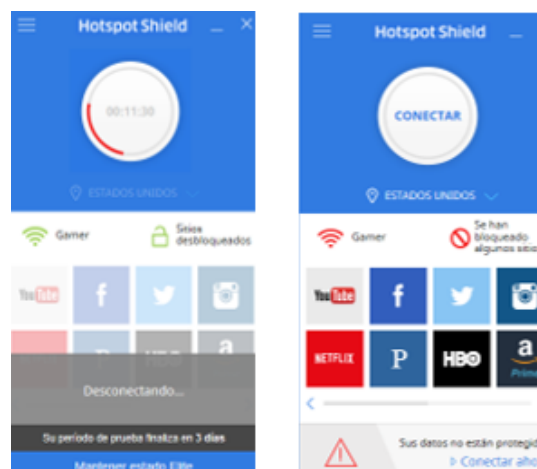


Figura 11. Menú hotspot shield. Figura 12. Menú hotspot shield.

6. Desconectar el software, ver figura 11 y 12, luego cerrar el software.

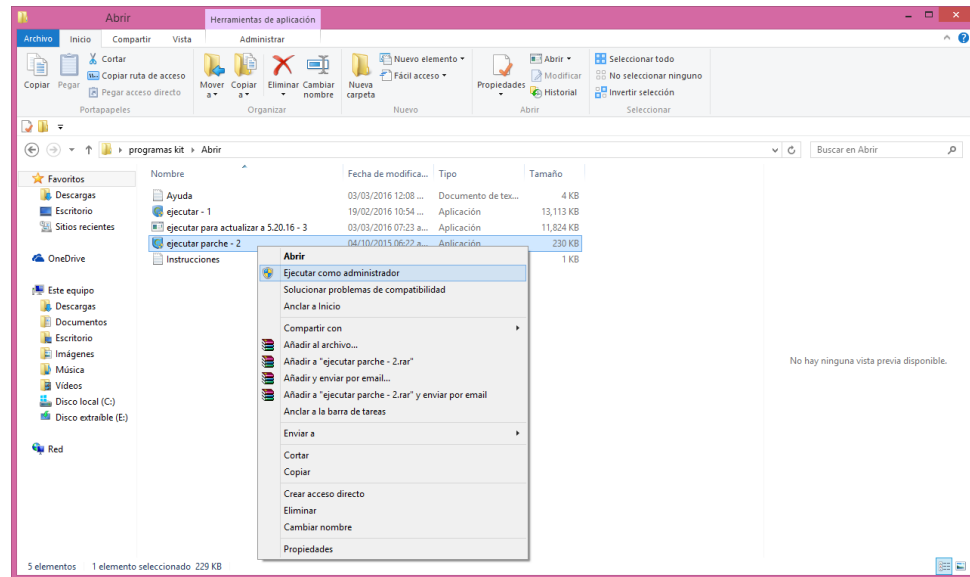


Figura 13. Parche para hotspot shield.

7. Ejecutar el parche con permisos de administrador, para activar el software. ver figura 13.

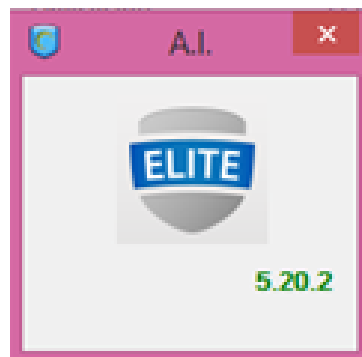


Figura 14. Parche.



Figura 15. Parche.

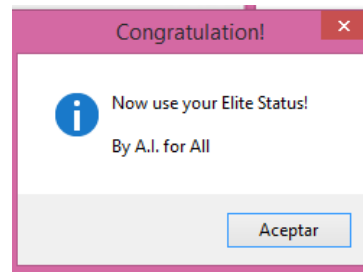


Figura 16. Parche.

8. Aparece este cuadro que es el parche, dar clic sobre el ver figura 14, empezará a cargarse ver figura 15. Una vez terminado saldrá un mensaje, dar clic en aceptar ver figura 16, y quedará activado. Se reinicia el software, y procedemos a actualizar a la versión elite.

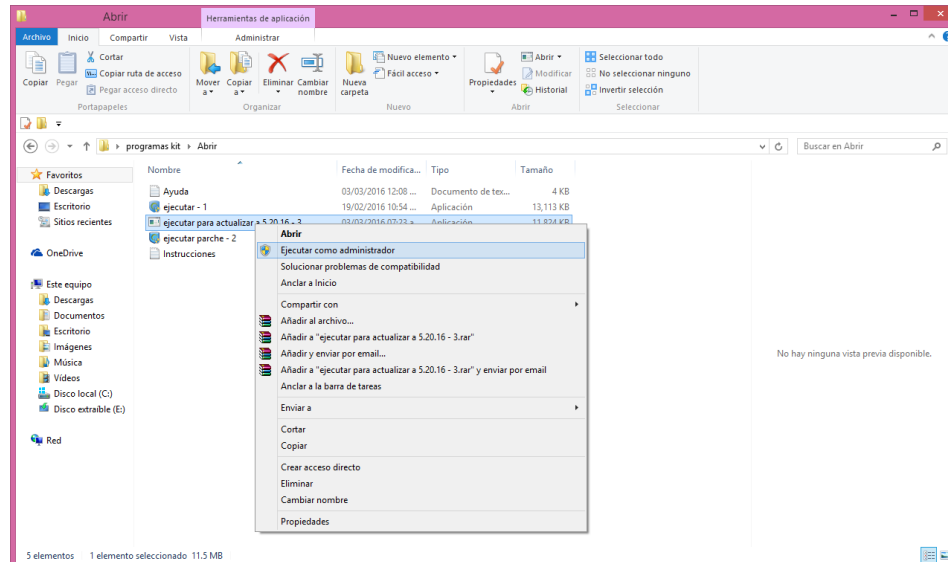


Figura 17. Actualizador.

9. Ejecutar el actualizador, a la versión elite con permiso de administrador, clic derecho y ejecutar como administrador, Ver figura 17.

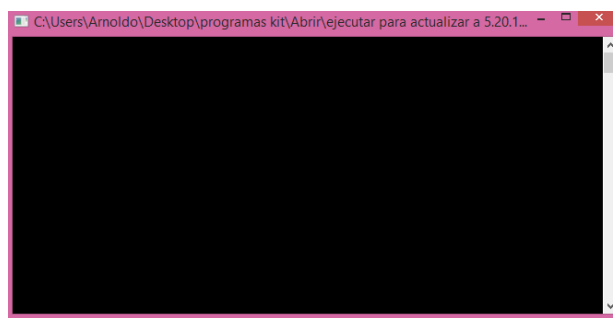


Figura 18. Actualizador.

10. Aparecerá este cuadro, ver figura 18 esperar unos 5 minutos, para que se actualice a la versión Elite.

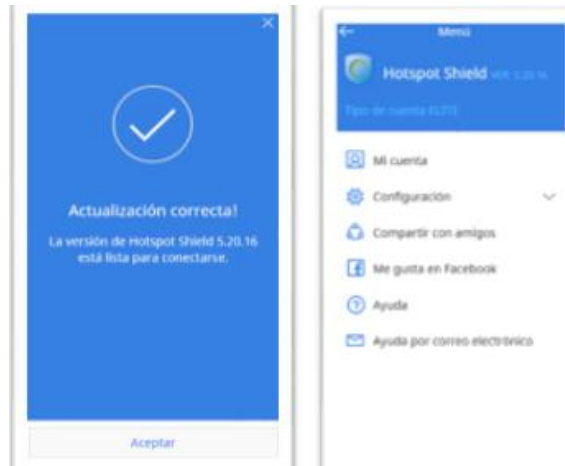


Figura 19. Menú hotspot shield. Figura.20. Menú hotspot shield.

11. Se iniciará el software automáticamente, aparece el cuadro siguiente ver figura 19, actualización correcta versión 5.20.16 lista para conectarse, verificamos en menú ver figura 20, y en efecto el tipo de cuenta es elite lista para utilizar.

Uso de Hotspot Shield.

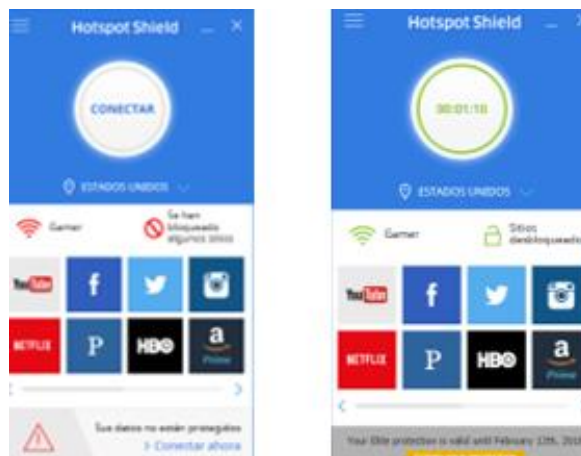


Figura 1. Menú.

Figura 2. Menú.

1. Antes que nada, conectar el software. Para ello clic sobre conectar ver figura 1, en uso de Hotspot Shield se observa que se ha conectado, ver figura 2.

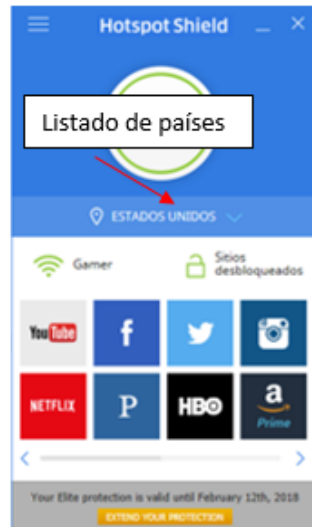


Figura 3. Lista de países.

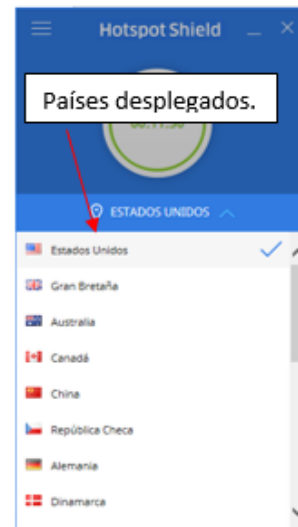


Figura 4. Lista de países.

2. Desplegar los diferentes países que viene con el software, son 20 países los cuales al dar conectar, navega con el país al que seleccione, ver figuras 3 y 4. En este caso Estados unidos.

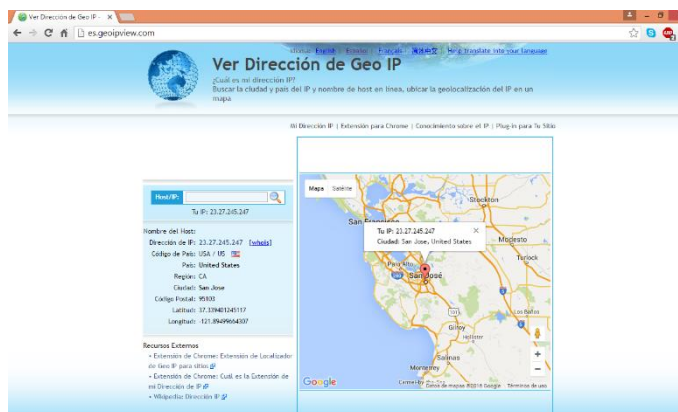


Figura 5. Página web.

3. Ingresar a la página <http://es.geoipview.com/>, verificar de donde se ha conectado. En efecto aparece San Francisco C.A, ver figura 5 se conecta a uno de los 20 países que necesite conectarse.

2.1.7 manual de instalación y uso AVG antivirus.

Nota: actualizar en informes el antivirus, para tener la versión completa free, y no aparezca que solo dura 30 días.

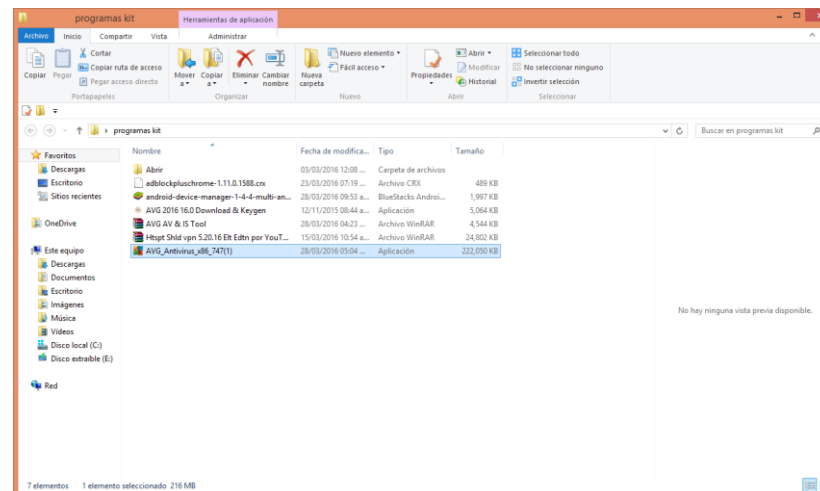


Figura 1. Instalador AVG.

1. ejecutar el antivirus, ver figura 1.

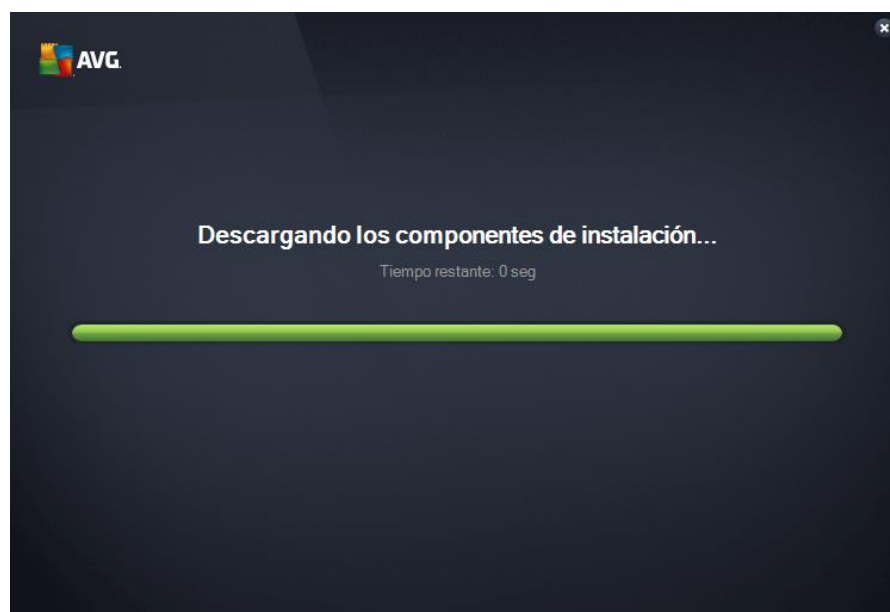


Figura 2. Instalador AVG.

2. En el siguiente cuadro, ver figura 2 esperar hasta que se descarguen los componentes necesarios del instalador.



Figura 3. Instalador AVG.

3. En el siguiente cuadro, ver figura 3. Elegir el idioma, español en este caso, y dar clic en instalar.



Figura 4. Instalador AVG.



Figura 5. Instalador AVG.

4. En el siguiente cuadro, ver figura 4 y 5. Esperar a que se descargue el software.

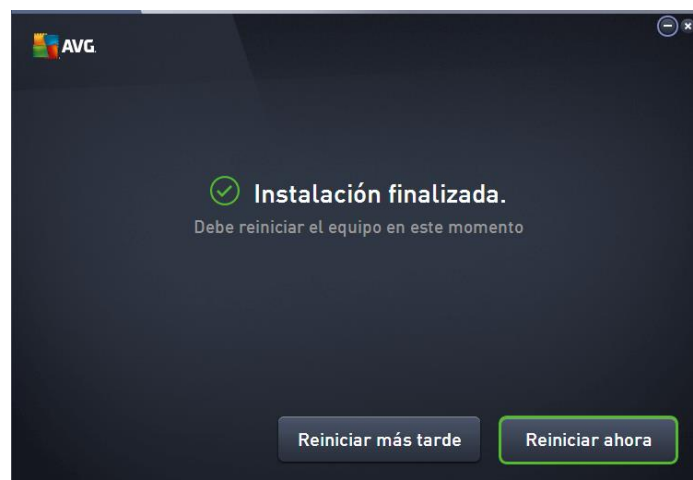


Figura 6. Instalador AVG.

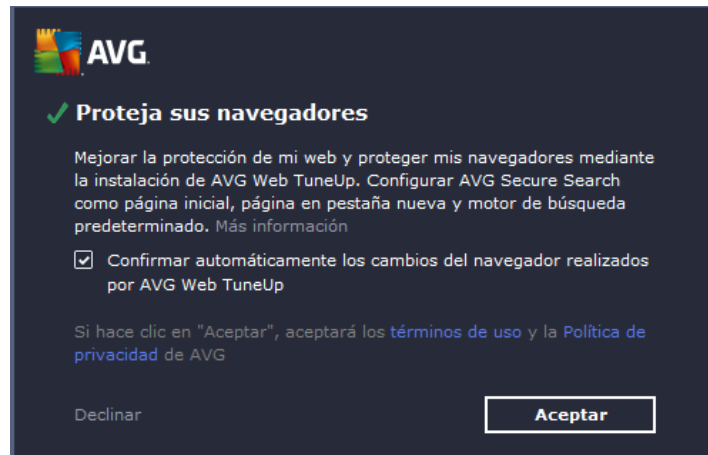


Figura 7. Nota emergente.

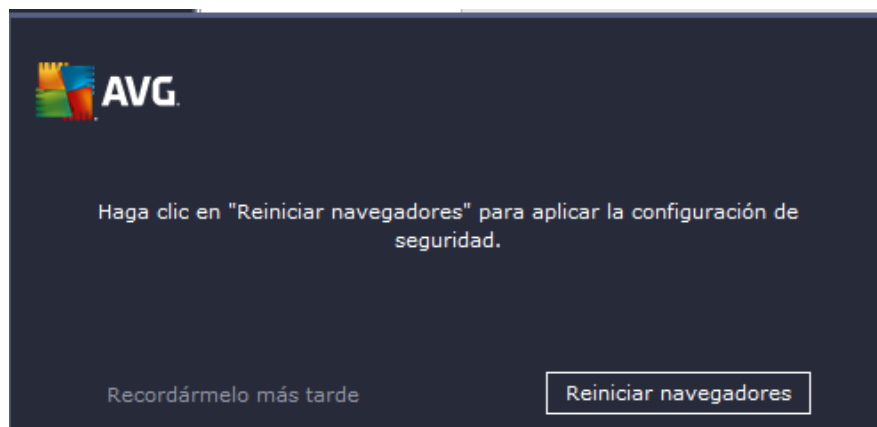


Figura 8. Nota emergente.

5. La instalación finalizó con éxito. Pedirá reinicio ver figura 6, además pedirá unos permisos adicionales, ver figura 7 aceptamos, y saldrá otra nota de reiniciar navegadores, para aplicar los cambios de seguridad a los navegadores que pidió anteriormente, en la figura 7 clic en reiniciar navegadores ver figura 8.

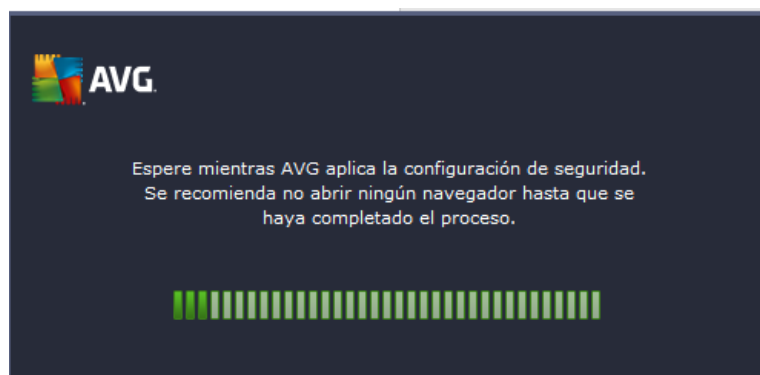


Figura 9. Nota emergente.

6. Esperar hasta que AVG aplique la configuración de seguridad, ver figura 9.

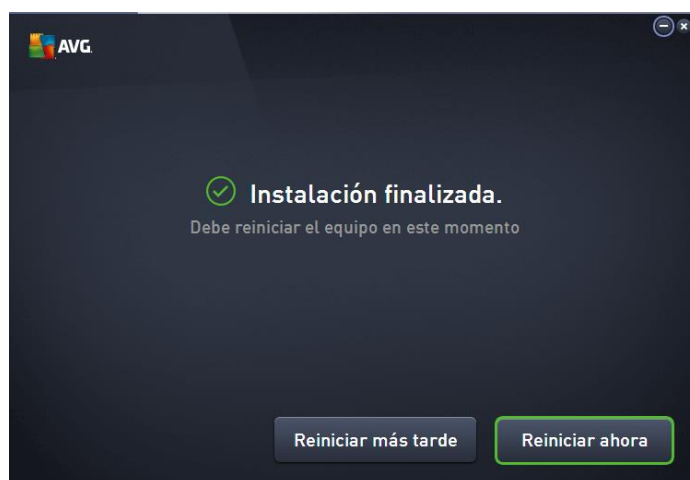


Figura 10. Instalador AVG finalizada.



Figura 11. Menú AVG.

7. Ahora sí, clic en reiniciar. Listo queda finalizado la instalación ya está lista para su uso, ver figura 11.

Uso de AVG Antivirus.



Figura 1. Menú AVG.

1. En el siguiente cuadro, ver figura 1. Es la interfaz del antivirus, con su respectivo menú.



Figura 2. Protección de equipo.

2. Clic en equipo, ver figura 1 y saldrá lo siguiente, ver figura 2 hay dos opciones, la primera: es para activar o desactivar el antivirus, la segunda: es una opción de caja fuerte de datos. Clic en crear caja fuerte.



Figura 3. Caja fuerte de datos.

3. Aparece lo siguiente, ver figura 3 y agregar los campos, una contraseña y una palabra clave para recordar la contraseña. Este sitio, almacenará los archivos que guardar en ella, y estará protegida habrá que ingresar la contraseña. Clic en siguiente.

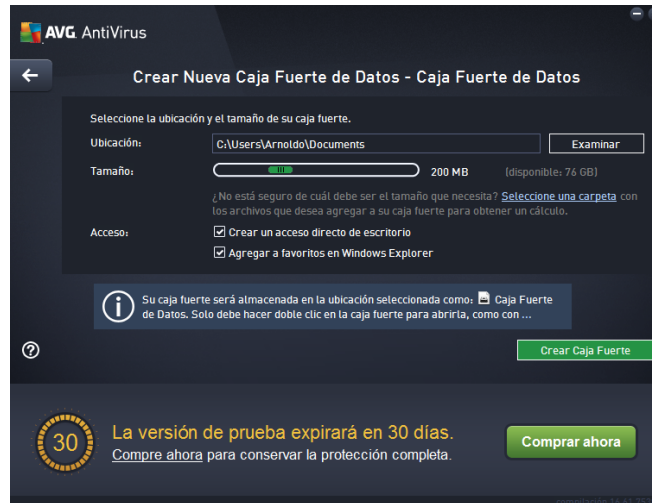


Figura 4. Caja fuerte de datos.

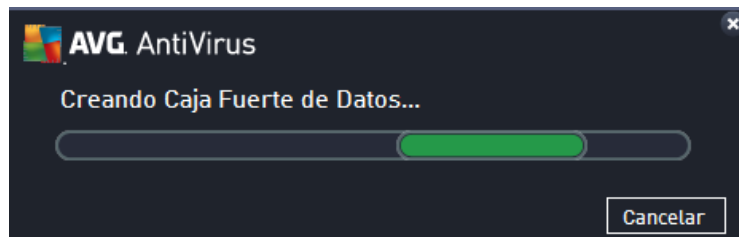


Figura 5. Caja fuerte de datos.

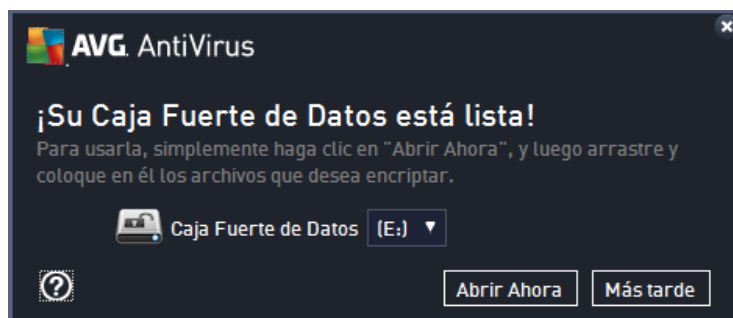


Figura 6. Caja fuerte de datos.

4. En el siguiente cuadro, ver figura 4 clic en aceptar para terminar de crear la caja fuerte, y saldrá un mensaje crear caja fuerte de datos, ver figura 5 y esperar hasta que

se termine de crear, al final confirmará con un mensaje su caja fuerte de datos esta lista, ver figura 6 y quedara lista para usarla.

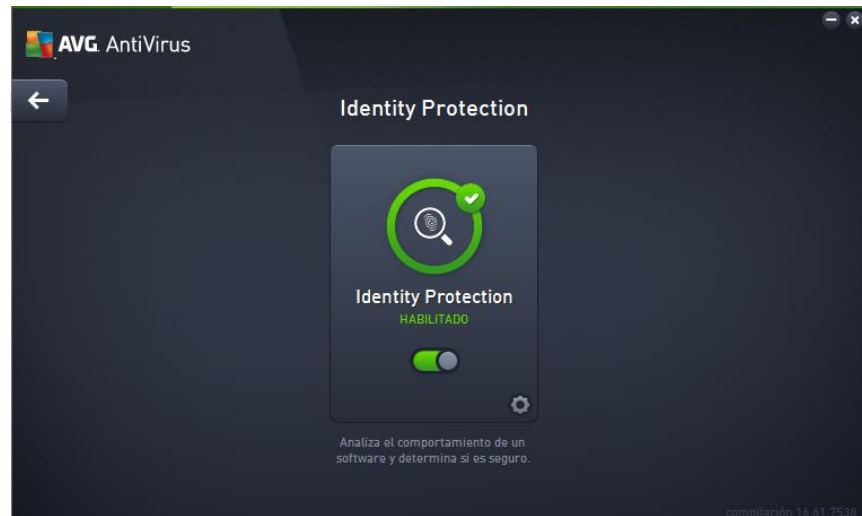


Figura 7. Identidad.

5. Clic en identidad, ver figura 1 y se despliega el siguiente menú, ver figura 7 de termina si es seguro un software, analiza el comportamiento.



Figura 8. Protección de correo electrónico.

6. Clic en email, ver figura 1 se desplegará el siguiente menú, ver figura 8. El primero es: la protección al correo electrónico para analizar para detectar correos dañinos la siguiente es: anti spam solo que esta solo está disponible si se tiene la versión de paga.



Figura 9. Menú Analizar.

7. Para un análisis completo, clic en analizar ahora, se encuentra ubicado en la parte izquierda de abajo, ver figura 9.

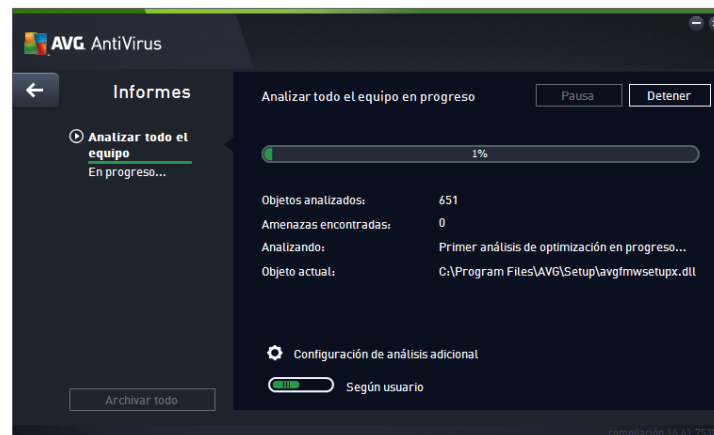


Figura 10. Menú Analizar.

8. Comenzará a analizar el equipo, esperar hasta que termine. ver figura 10.

2.1.8 manual de instalación y uso de malwarebytes.

Software que detecta y elimina aparte de Malware, gusanos, troyanos, bots, etc. Software para la detección de malware y compatible con la mayoría de los principales antivirus.

Nota: El siguiente software será utilizado: para activarlo con un parche y un serial, para ser utilizado para fines educativos enfocado a la enseñanza de cómo manejar herramientas para la protección de los equipos.

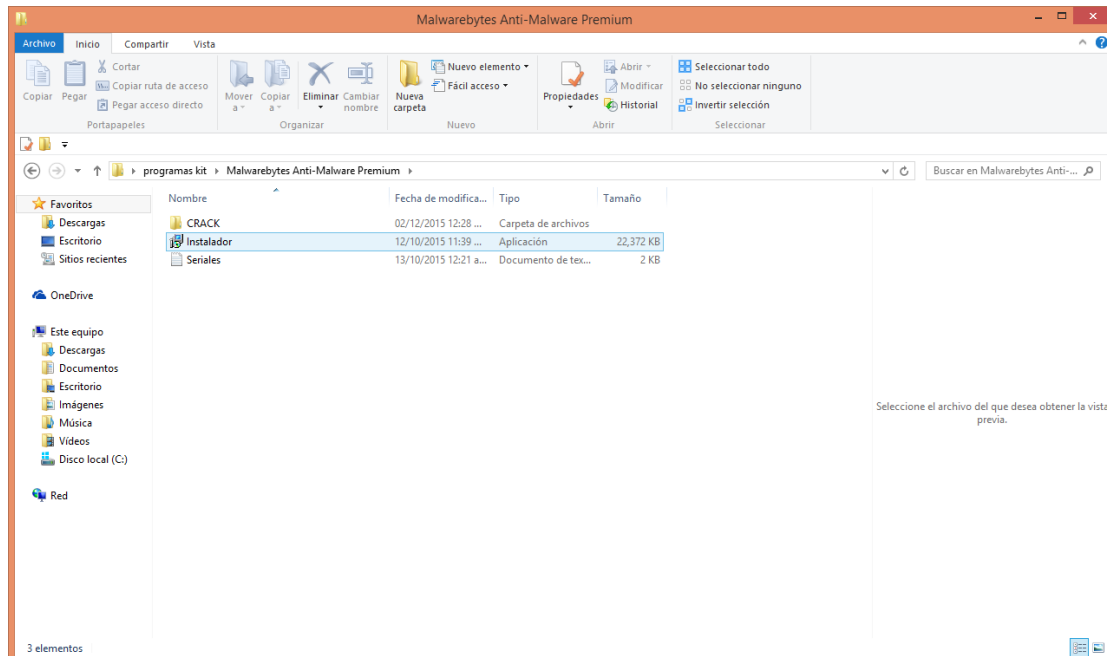


Figura 1. Instalador Malware bytes.

1. Ejecutamos el instalador, Malware bytes ver figura 1.

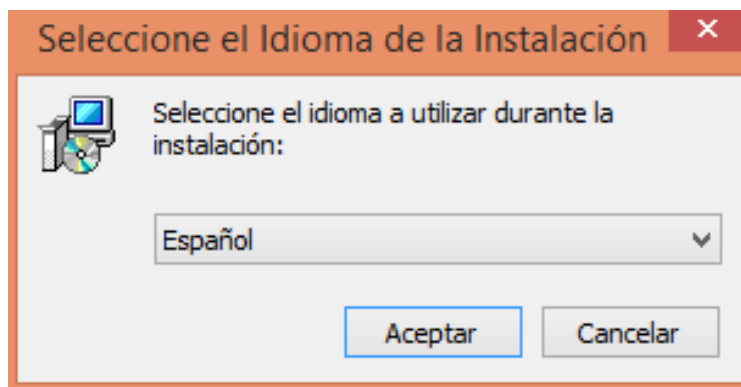


Figura 2. Instalador Malware bytes.

2. Emerge el siguiente cuadro, ver figura 2 elegir el idioma en este caso en español, y damos clic en aceptar.



Figura 3. Instalador Malware bytes.

3. En el siguiente cuadro, ver figura 3 es el asistente de instalación, clic en siguiente.



Figura 4. Instalador Malware bytes.

4. Aceptar los términos de la licencia dar clic en “acepto el acuerdo” y clic en siguiente.

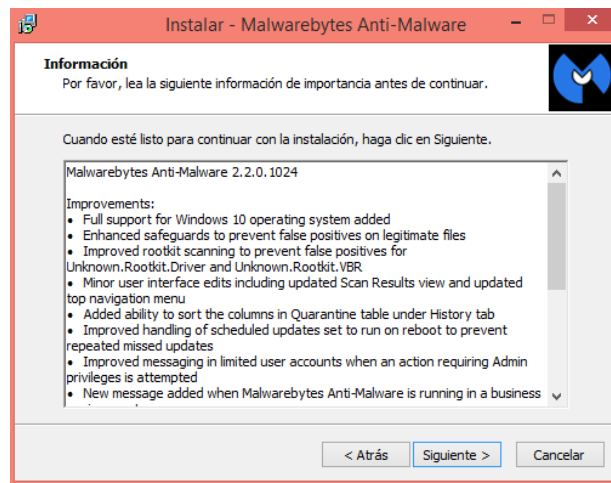


Figura 5. Instalador Malware bytes.

5. Clic en siguiente nueva mente, ver figura 5.

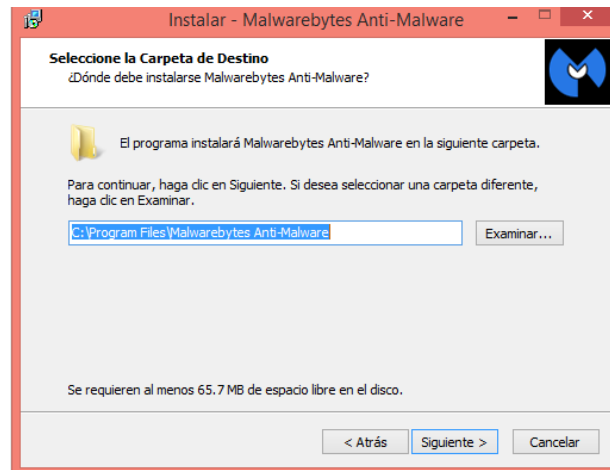


Figura 6. Instalador Malware bytes.

6. En el cuadro siguiente, ver figura 6 elegir el lugar donde se instalen los archivos del Malwarebytes, se recomienda dejarlo por defecto donde indica, pero si es posible guardarlo en otro lugar, una vez listo dar clic en siguiente.

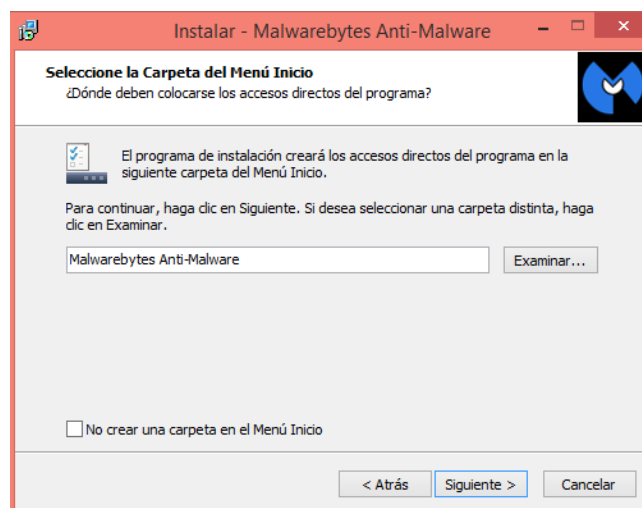


Figura 7. Instalador Malware bytes.

7. En el cuadro siguiente, ver figura 7 dar clic en siguen, instalará accesos directos del software.

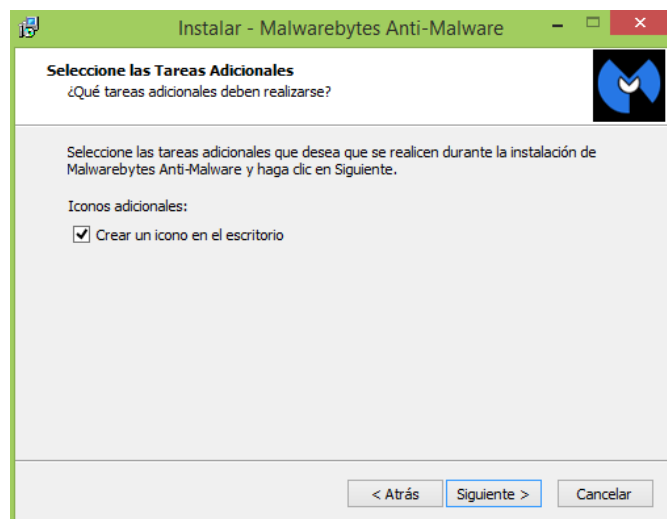


Figura 8. Instalador Malware bytes.

8. En el siguiente cuadro, ver figura 8. Clic en siguiente, creará un acceso directo en el escritorio.

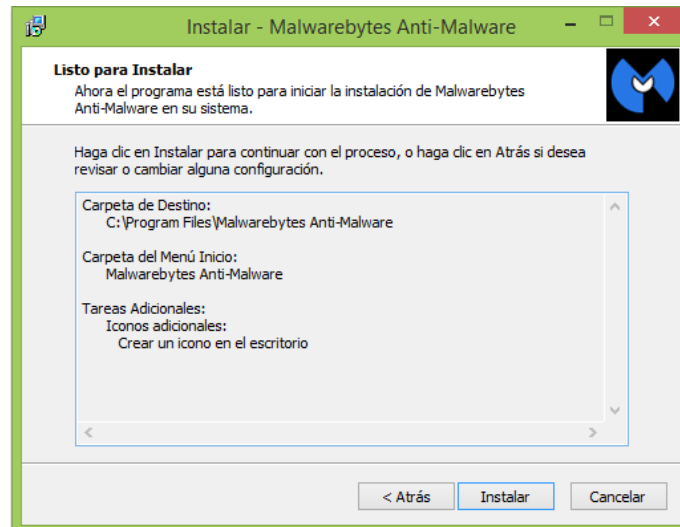


Figura 9. Instalador Malware bytes.

9. Ya para instalar, ver cuadro 9. Clic en instalar.

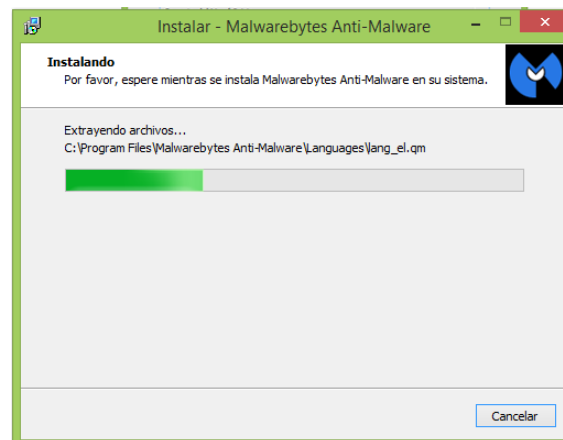


Figura 10. Instalador Malware bytes.

10. Esperar que termine de instalar.



Figura 11. Fin de Instalación Malware bytes.

11. Para terminar, ver figura 11 ya termino de instalarse, y desmarcamos la casilla donde dice ejecutar Malwarebytes anti-malware, clic en finalizar.

Parchando el software.

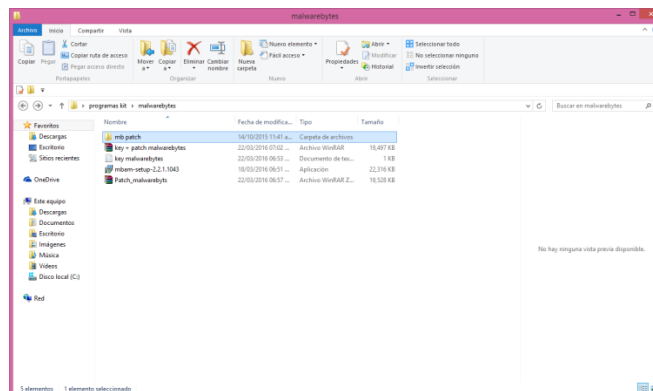


Figura 1. Parche Malware bytes.

1. Abrir la carpeta parche.

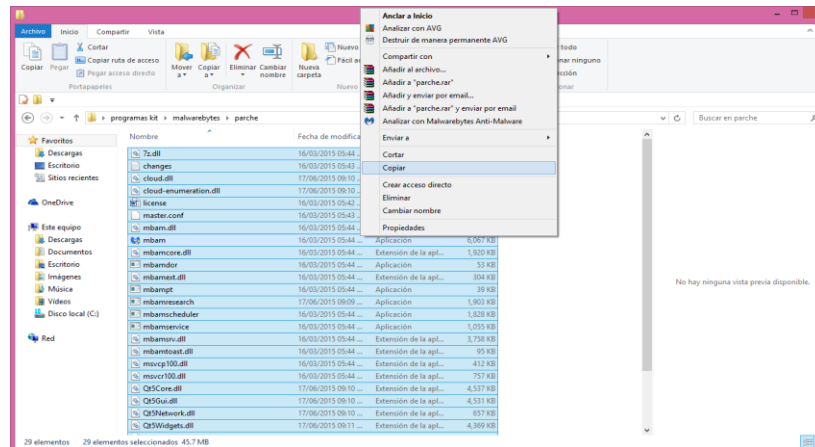


Figura 2. Parche Malware bytes.

2. Seleccionar todos los archivos, control + E y clic derecho copiar.

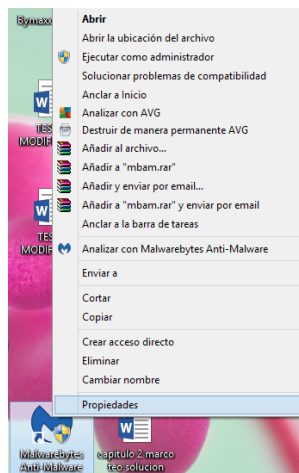


Figura 3. Acceso directo Malware bytes.

3. Ubicar el acceso directo de Malwarebyte, clic derecho y clic en propiedades ver figura

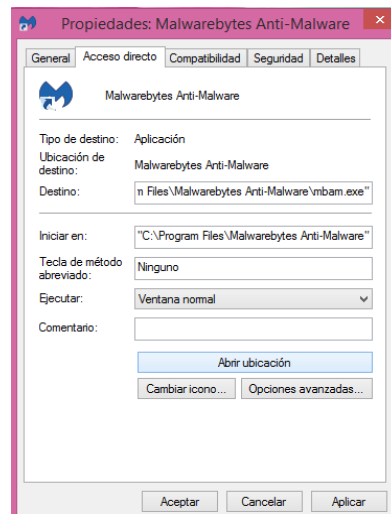


Figura 4. Propiedades.

4. En propiedades, dar clic en abrir ubicación, ver figura 4.

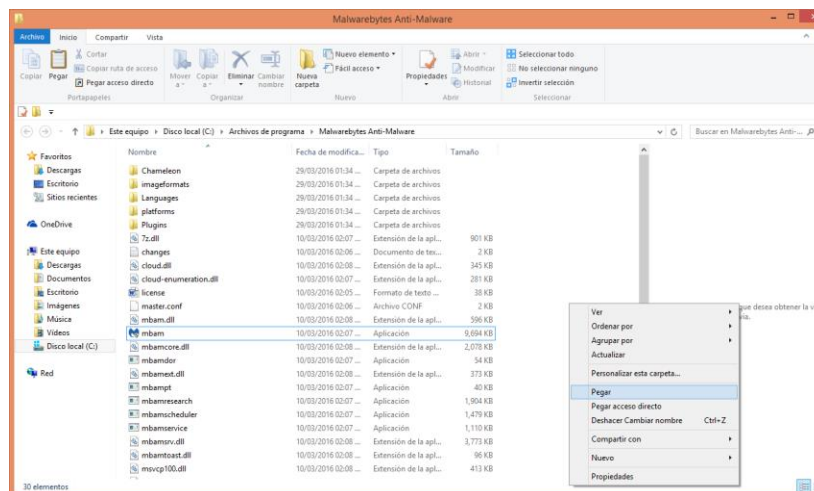


Figura 5. Carpeta de archivos de Malware bytes.

5. Aparecen los archivos de malwarebytes, y dar clic derecho pegar.

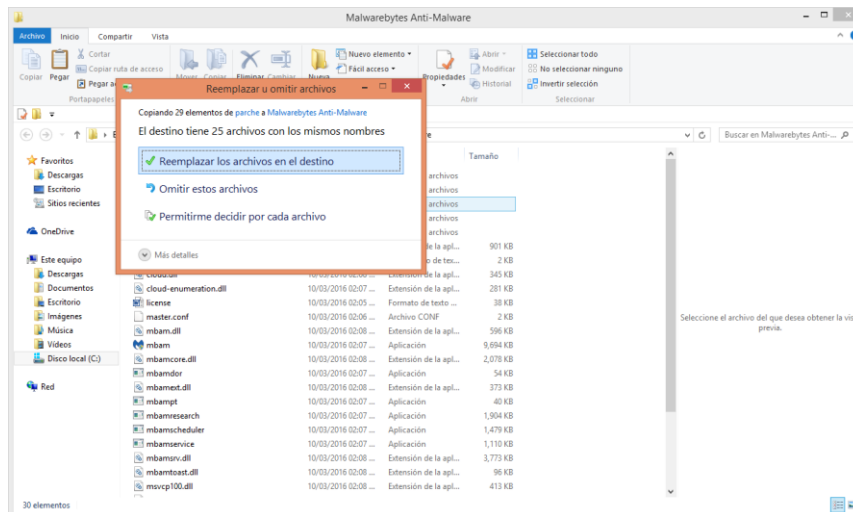


Figura 6. Carpeta de archivos de Malware bytes.

6. Aparece el siguiente mensaje, ver figura 6 hacer clic donde dice reemplazar los archivos en el destino.

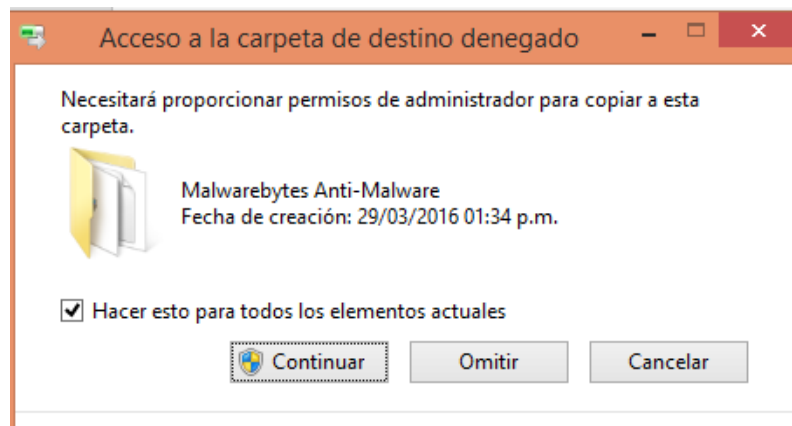


Figura 7. Ventana emergente.

7. Emergerá este mensaje, ver figura 7, marcar la casilla hacer esto para todos los elementos, hacer clic sobre continuar.

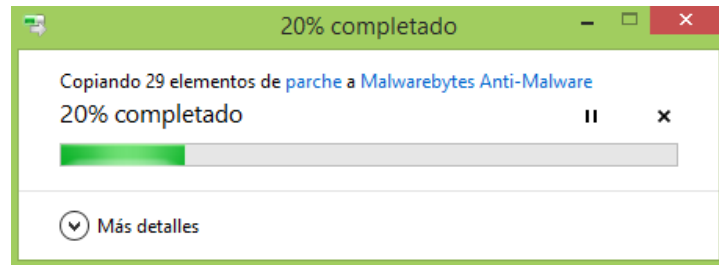


Figura 8. Copiando archivos.

8. Se copian los Archivos, esperar y cerrar todo cuando se termine de copiar.

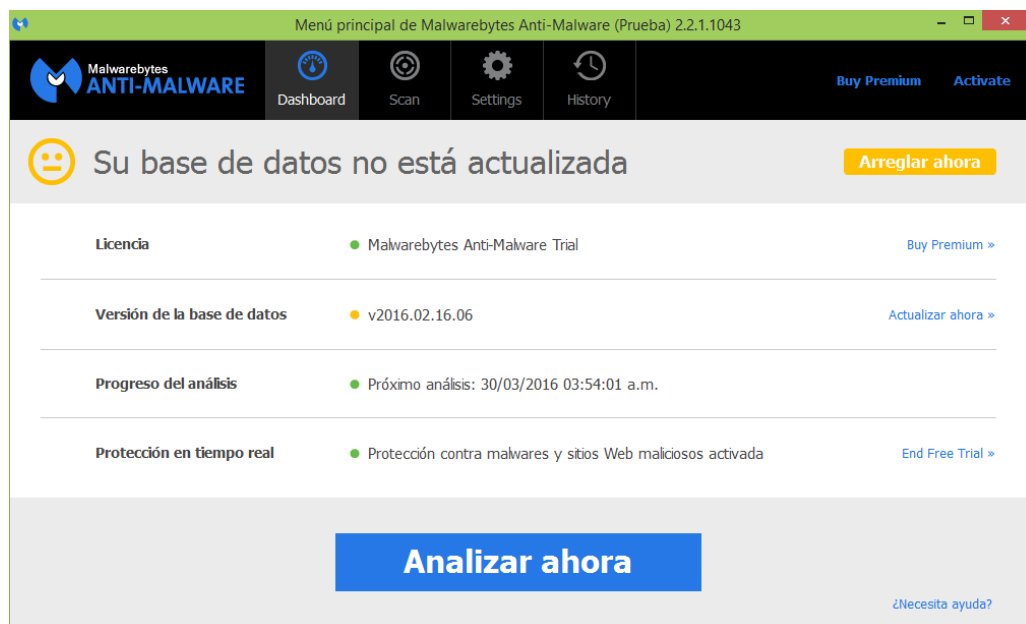


Figura 9. Menú Malwarebytes.

9. Abrir el Malwarebytes, y dar clic en activar.

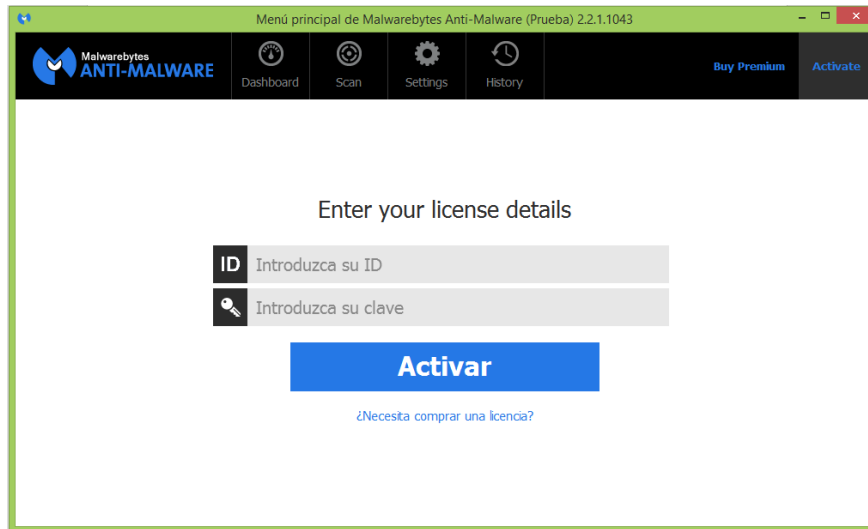


Figura 10. Activador de Lincensia.

10. En el siguiente cuadro, ver figura 10 ingresar una ID y una clave.

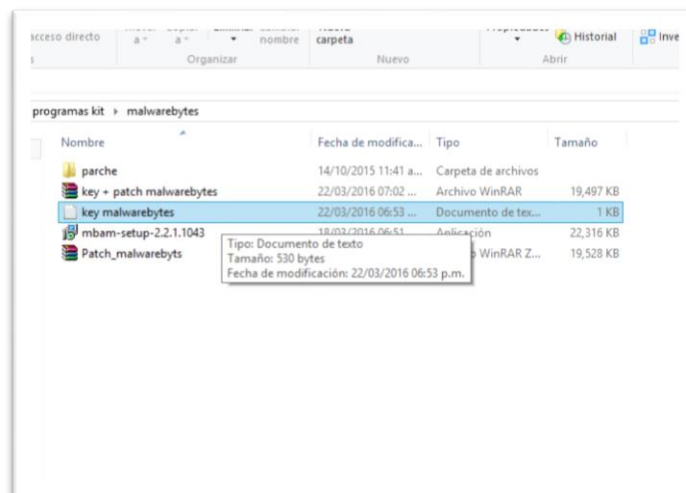


Figura 11. Bloc de nota con Claves para Malwarebytes.

11. Abrir Key Malwarebytes ver figura 11.

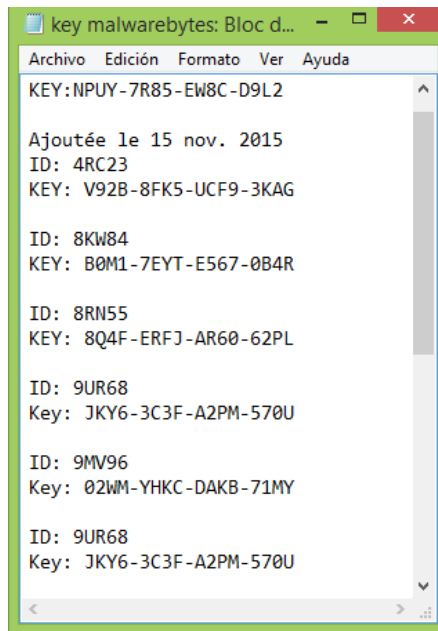


Figura 12. Calves para Malwarebytes.

12. En el siguiente cuadro, ver figura 12 estarán algunas ID y clave, copiar y pegar.

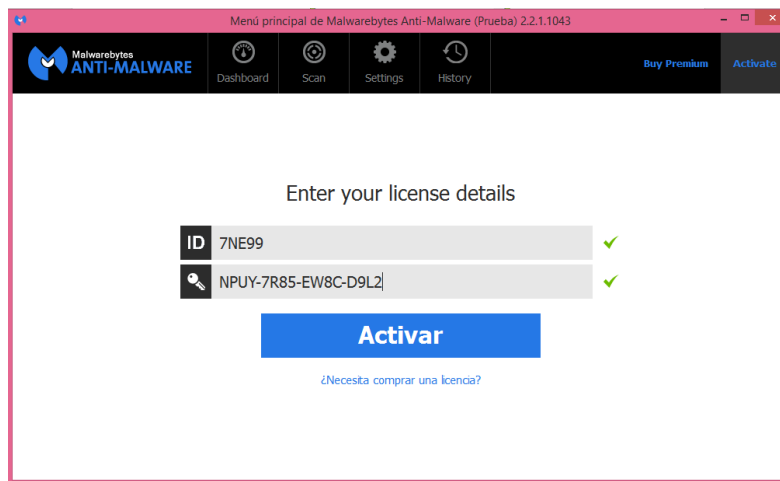


Figura 13. Activador de Lincensia.

13. En el siguiente cuadro, ver figura 13 y pegar la ID y clave fue aceptado está en verde el chequcito, clic en activar.

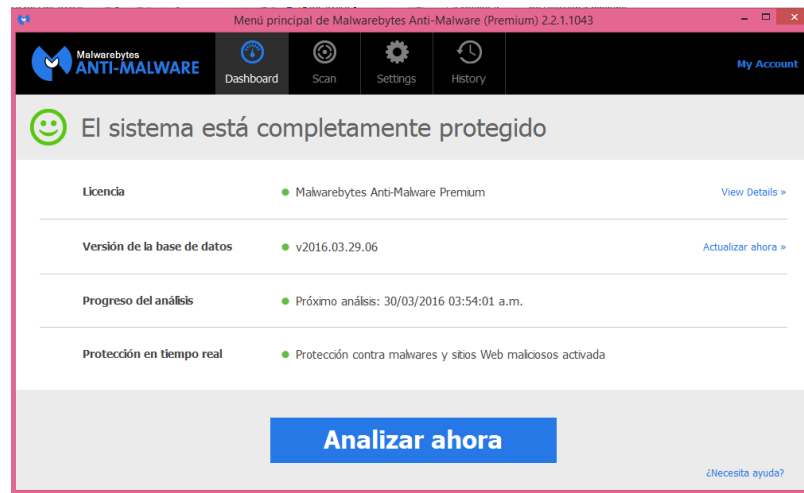


Figura 14. Verificando si está activado

14. El software Malwarebytes, queda totalmete activado listo para utilizarse.

Uso de Malwarebytes.

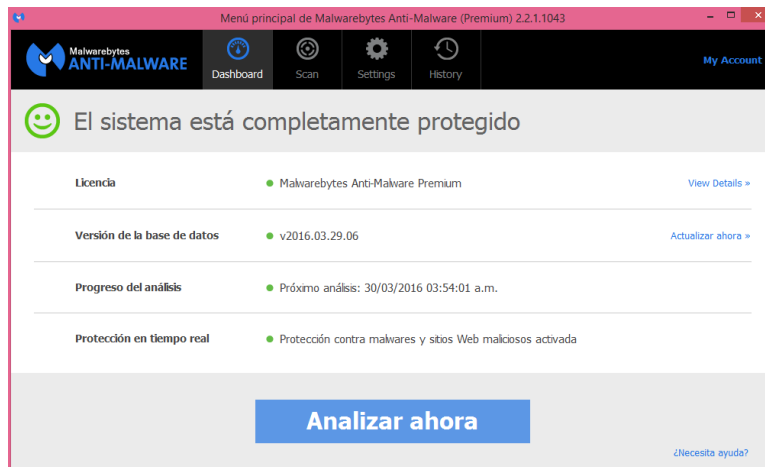


Figura 1. Menú malwarebytes.

1. Para comenzar a utilizar malwarebytes, aparece el menú principal, clic en analizar ahora ver figura 1.

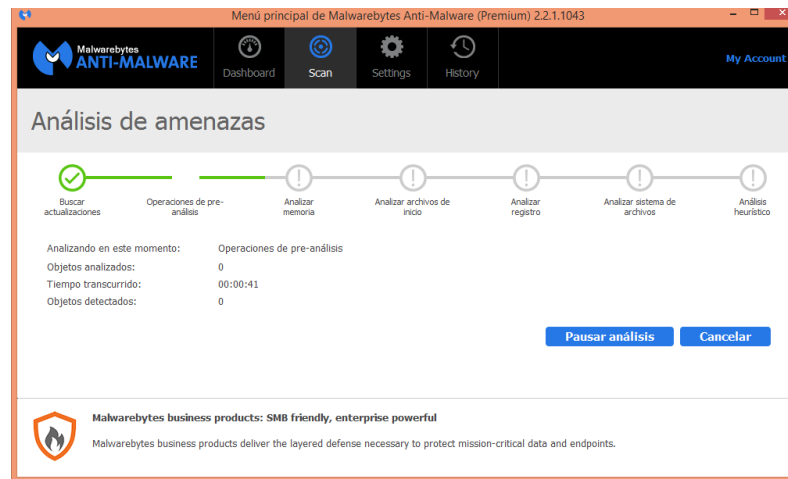


Figura 2. Análisis de amenaza.

2. Ver figura 2, comenzara el análisis esperar hasta que termine.

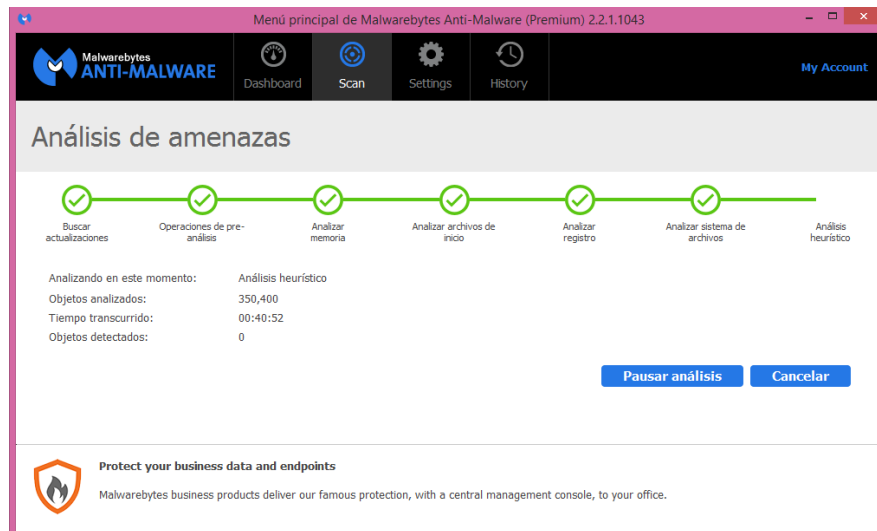


Figura 3. Análisis de amenaza.

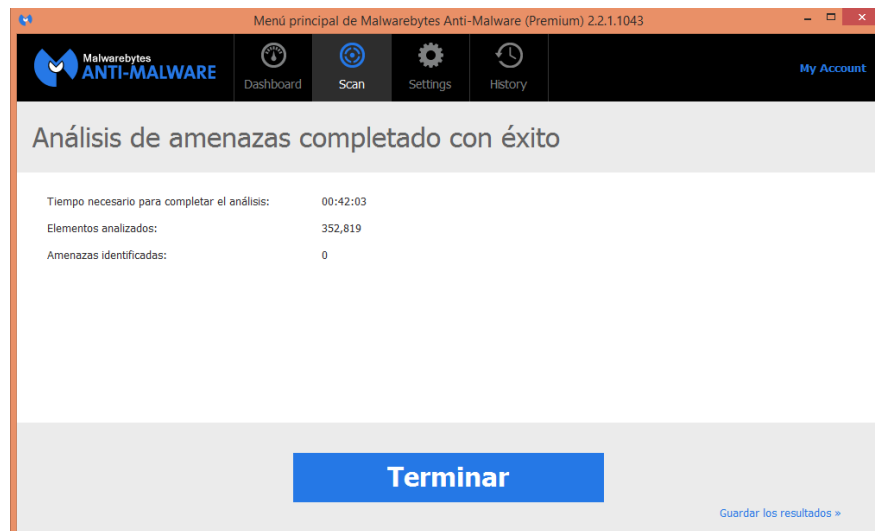


Figura 4. Análisis de amenaza.

3. Una vez terminado el análisis, ver figuras 3 y 4. Aparece tiempo necesario para completar el análisis, elementos analizados y por último amenazas identificadas, en este caso no se encontraron amenazas, clic en terminar y automáticamente vuelve al menú inicial del software.



Figura 5. Análisis.

4. Dar clic en Scan y aparece lo siguiente, ver figura 5

- análisis de amenaza: Es el recomendado, ya que analiza profundo todos los sectores del pc.
- Análisis personalizado: Su función es elegir dónde, y que se desea analizar.
- análisis rápido: Comprueba rápidamente su sistema, en busca de amenazas de malware activas, si no se encuentran amenazas se recomienda usar análisis de amenazas ya que es más efectiva.

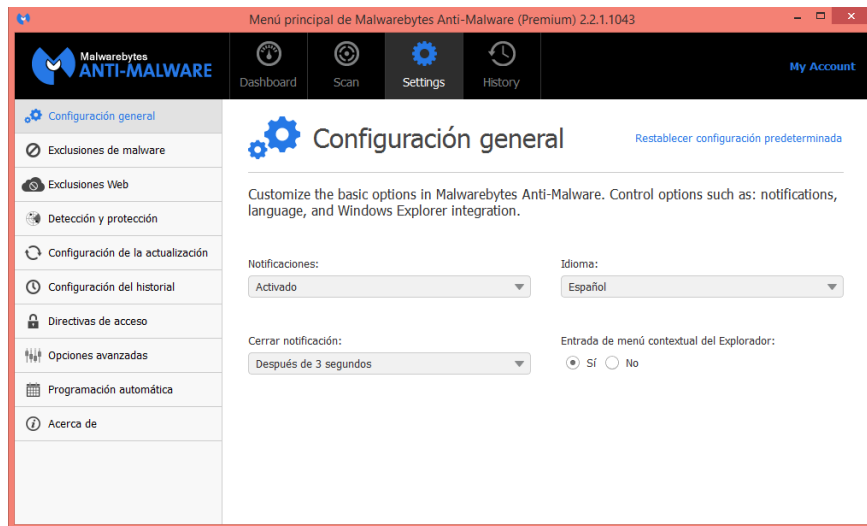


Figura 6. Configuración general.

5. En el siguiente cuadro, ver figura 6 clic en settings aparece la configuración general.

Se recomienda dejarlo de fábrica para no tener problemas de rendimiento del software.

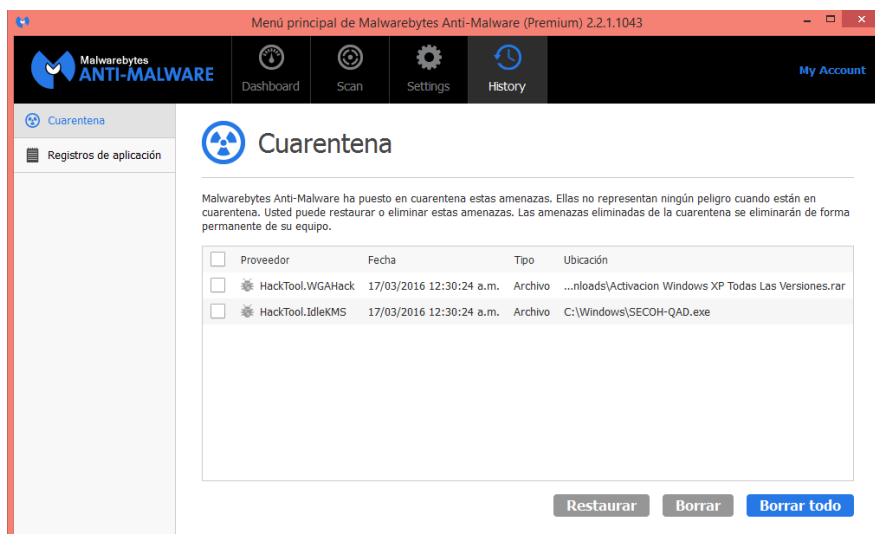


Figura 6. Virus en cuarentena.

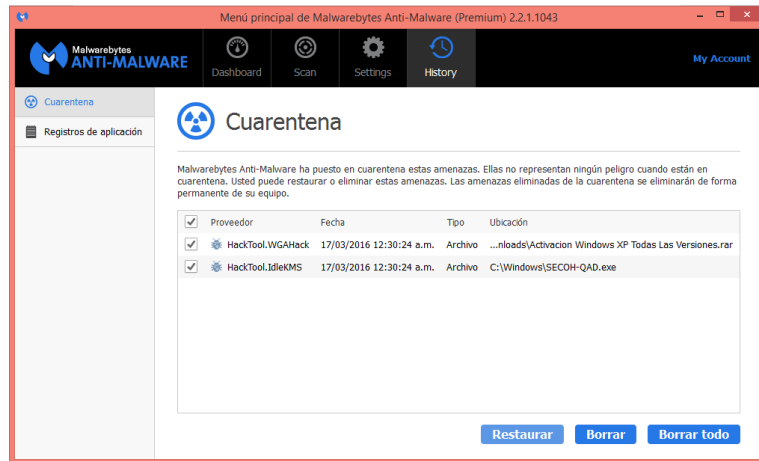


Figura 7. Virus en cuarentena.

6. En el siguiente cuadro, ver figura 6 clic en History. Están la lista de amenazas puestas en cuarentena, en este caso hay dos, las podemos eliminar totalmente o si saben que no son amenazas los pueden restaurar, solo hacer clic en la amenaza y elegir una de las 3 opciones, ver figura 7.

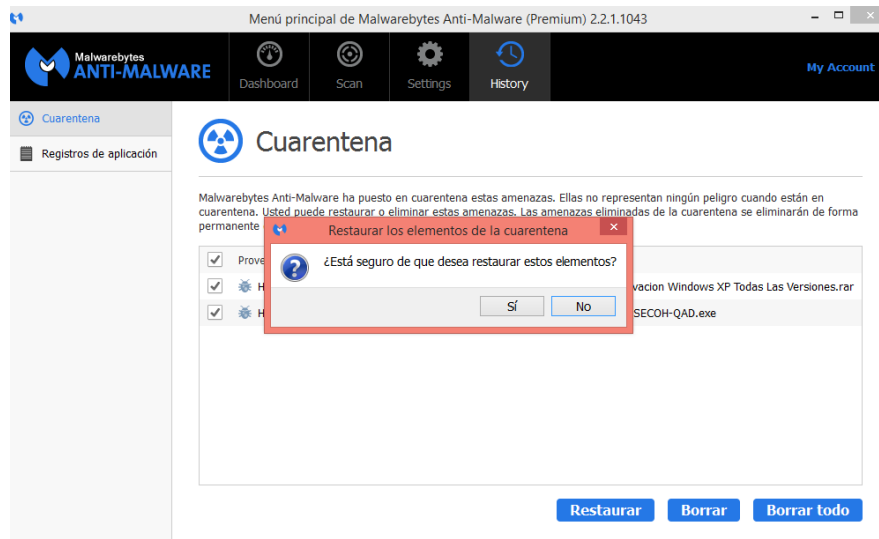


Figura 8. Virus en cuarentena.

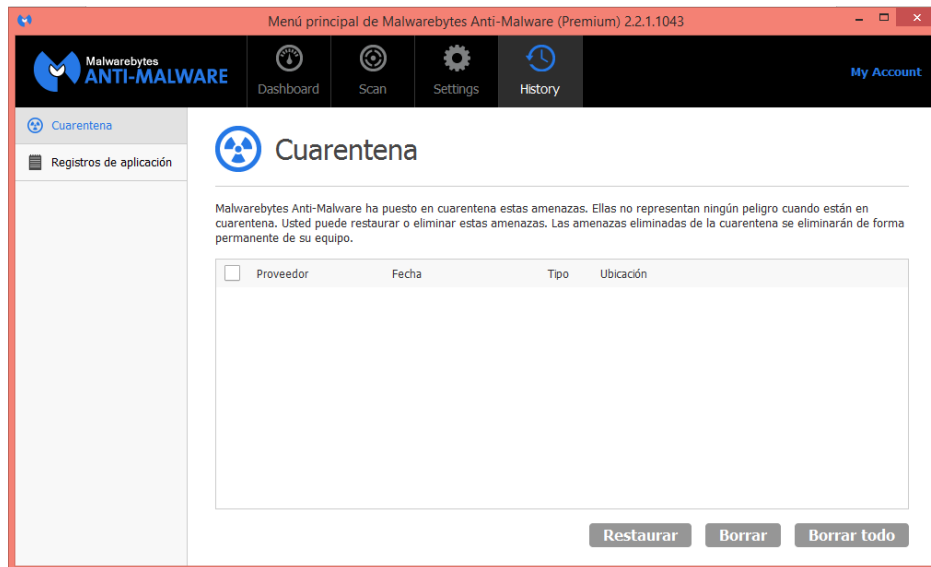


Figura 9. Virus en cuarentena.

7. Ver figura 8, en este caso restaurar las dos amenazas que detecto, porque realmente no son amenazas, son activadores de Windows que los detecto como amenazas, aparecerá un mensaje de confirmación que si está seguro de restaurar los archivos clic en sí y se restauran ver figura 9.

2.1.9 manual de instalación y uso de Comodo firewall.

Firewall personal que protege contra ataques de hackers o cualquier otro tipo de software malintencionado, controla aplicaciones que puedan tener acceso a internet y controlar las conexiones no autorizadas hacia y desde internet.

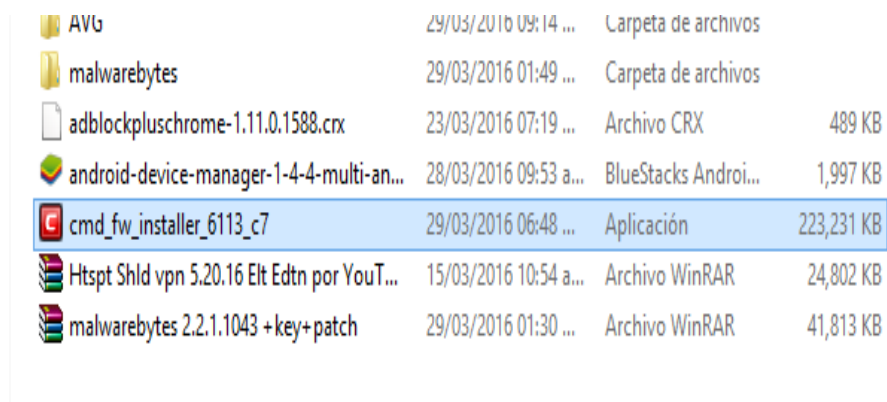


Figura 1. Instalador comodo firewall.

1. Ejecutar el instalador ver figura 1.

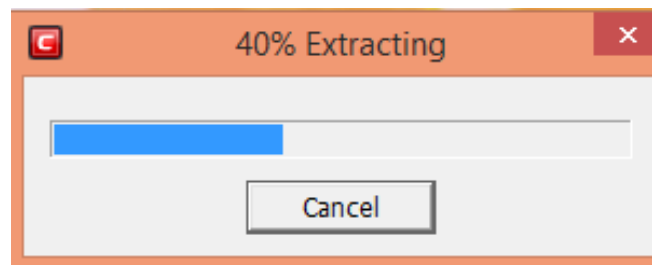


Figura 2. Instalador comodo firewall.

2. Saldrá el siguiente cuadro, ver figura 2 empezará a extraerse el software para iniciar instalación.

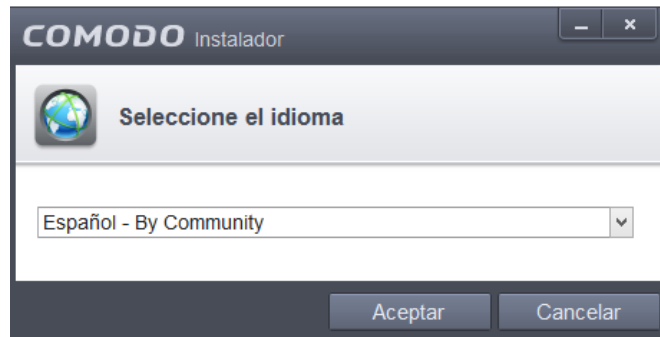


Figura 3. Instalador comodo firewall.

3. En el siguiente cuadro, ver figura 3 elegimos el idioma y clic en aceptar.



Figura 4. Instalador comodo firewall.

4. En el siguiente cuadro, dar clic en siguiente.



Figura 5. Instalador comodo firewall.

5. En el siguiente cuadro, ver figura 5 desmarcamos la segunda opción, y clic en aceptar e instalar.



Figura 6. Instalador comodo firewall.

6. Esperamos hasta que se instale, ver figura 6.



Figura 7. Menú principal de comodo firewall.

7. Una vez instalado saldrá el siguiente cuadro, ver figura 7 listo para utilizarlo.

Uso de Comodo Firewall.



Figura 1. Menú principal de comodo firewall.

1. En el siguiente cuadro, ver figura 1 en el uso de comodo firewall, tenemos el menú principal para comenzar a utilizarlo, dar clic en analizar en la parte de abajo.

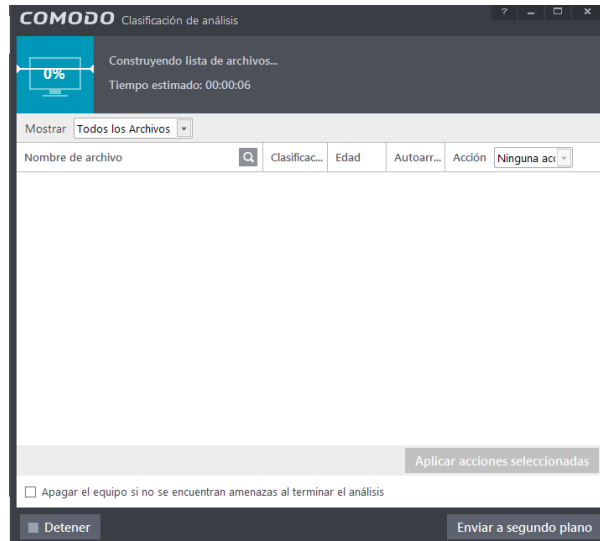


Figura 2. Comenzar analizar.

2. Comenzará el análisis, esperar hasta que termine de analizar en busca de archivos maliciosos.

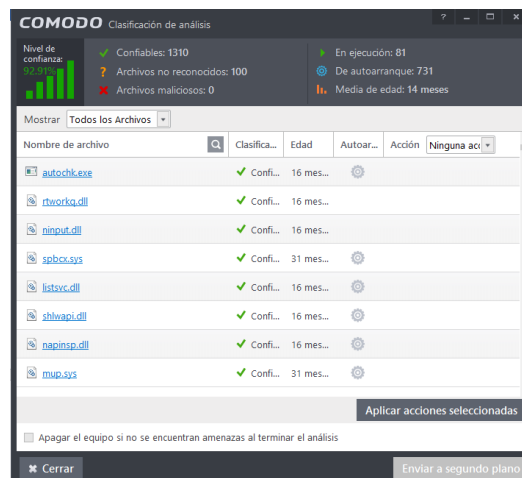


Figura 3. Analizando en busca de virus.

3. Ver figura 3, en este caso no encontró amenazas solo archivos confiables clic en cerrar.

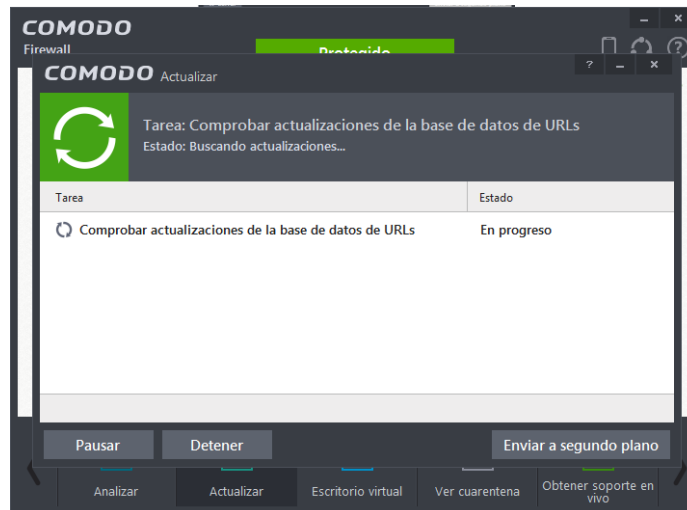


Figura 4. Analizando en busca de virus.

4. Clic en el siguiente icono, en la parte de abajo donde dice actualizar, ver figura 4 en esta parte busca si hay actualizaciones del software, si hay alguna automáticamente se actualiza solo es cuestión de aceptar e instalar, cuando termina de descargar los archivos en este caso no porque esta actualizado.



Figura 5. Analizando en busca de virus.

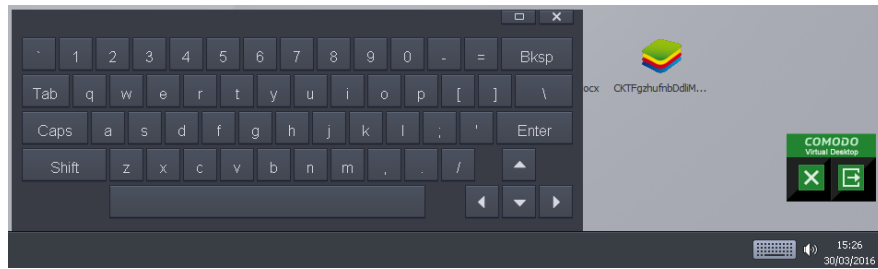


Figura 6. Teclado virtual.

5. Ver figura 5, dar clic en el siguiente icono, en la parte de abajo y se desplegará un teclado virtual, que su descarga es opcional si se desea usar, ver figura 6.

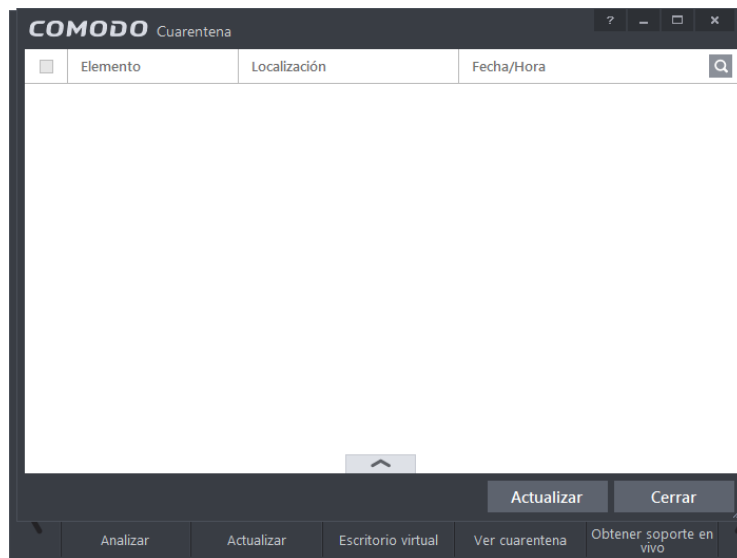


Figura 7. Archivos en cuarentena.

6. Hacer clic en cuarentena, en la parte del menú principal abajo y se desplegará el listado de las amenazas enviadas a cuarentena, ver figura 7 en este caso no hay ninguna amenaza.

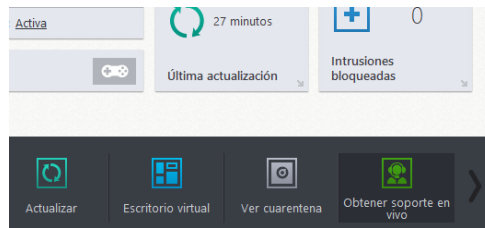


Figura 8. Soporte en línea.

7. En el siguiente cuadro, ver figura 8 aparece el ultimo icono que es para dar soporte en línea, si tienen algún problema podrán brindar ayuda.

2.1.10 manual de instalación y uso free vpn proxy.

Nota: Esta aplicación será instalada en dispositivos Android versión 4.0 o superior, en este caso se usará un emulador de dispositivos Android para la instalación, el proceso viene siendo el mismo en un dispositivo Android.

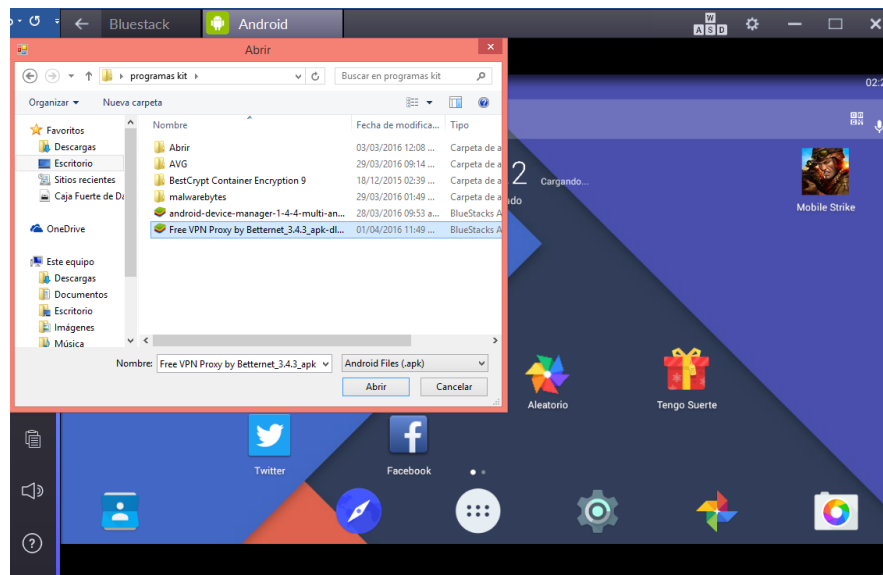


Figura 1. APK free VPN proxy.

1. Ejecutar Free VPN proxy, ver figura 1.

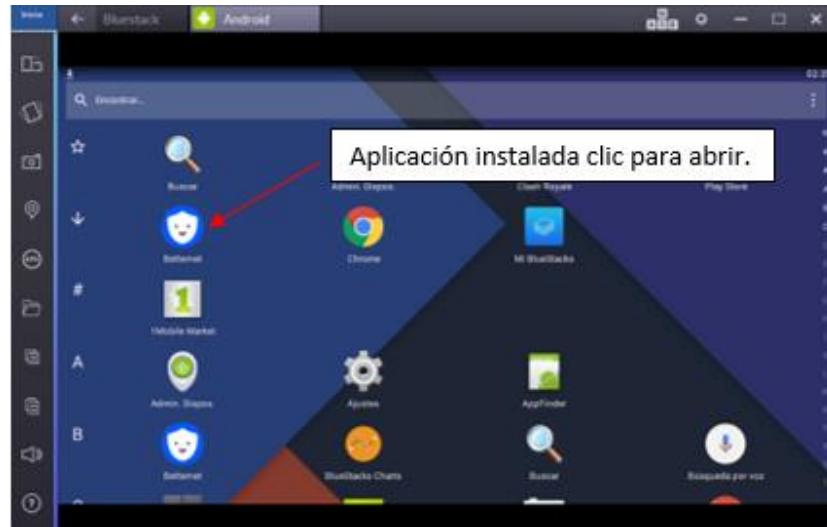


Figura 2. Aplicación instalada.

2. La aplicación se instaló con éxito, ya está lista para utilizar.

Uso de free VPN proxy.

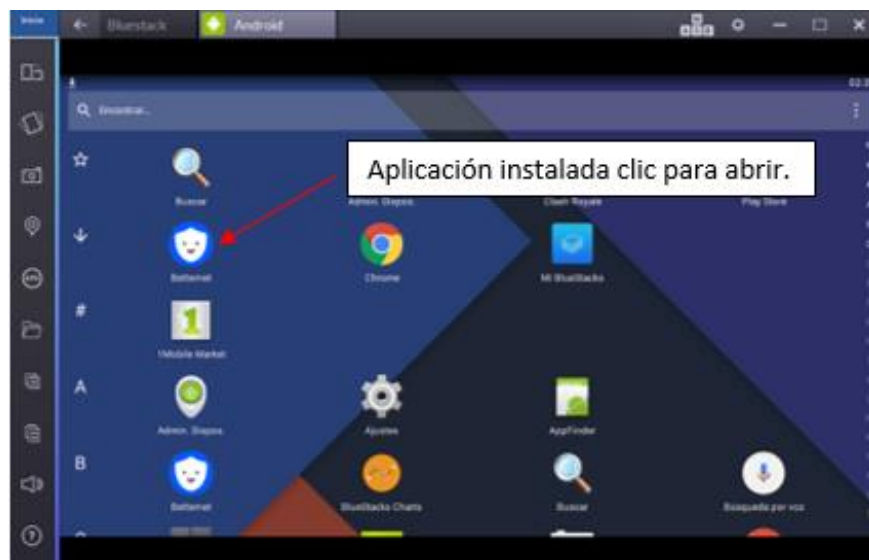


Figura 1. Aplicación instalada.

1. Clic para abrir la aplicación, ver figura 1 en usos de free VPN proxy.

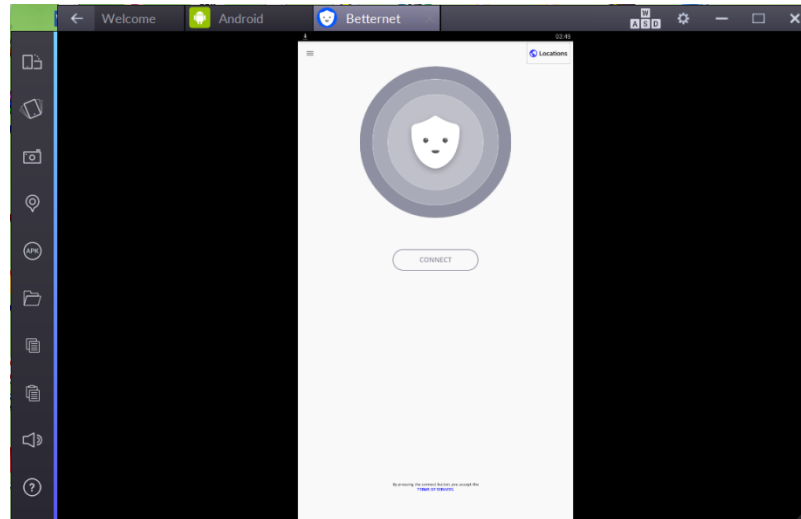


Figura 2. Free VPN proxy.

2. Dar clic en conectar, para empezar a utilizar la aplicación.

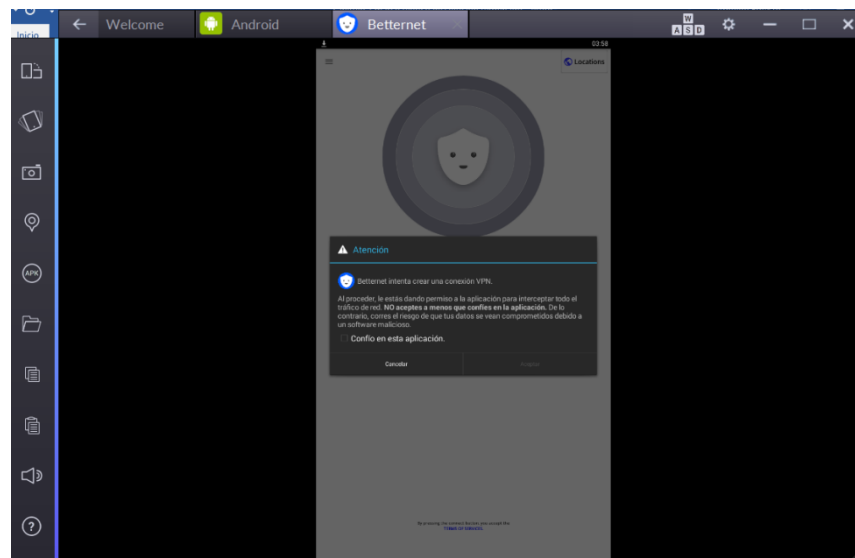


Figura 3. Free VPN proxy.

3. En el siguiente cuadro, ver figura 3 aceptamos el mensaje de permisos de la aplicación, clic en confió en esta aplicación, y clic en aceptar.

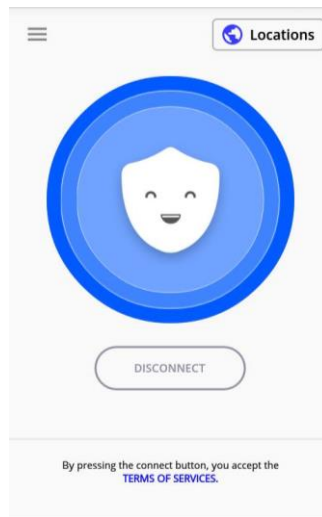


Figura 4. Free VPN proxy.

4. Se habrá conectado, ver figura 4 y estará haciendo su función la aplicación.

2.1.11 manual de instalación y uso bestcrypt container encryption.

Tipo de software que se utiliza para la encriptación de datos y carpetas en contenedores cifrados para la protección de los datos que pueda ser confidencial o importante para el usuario.

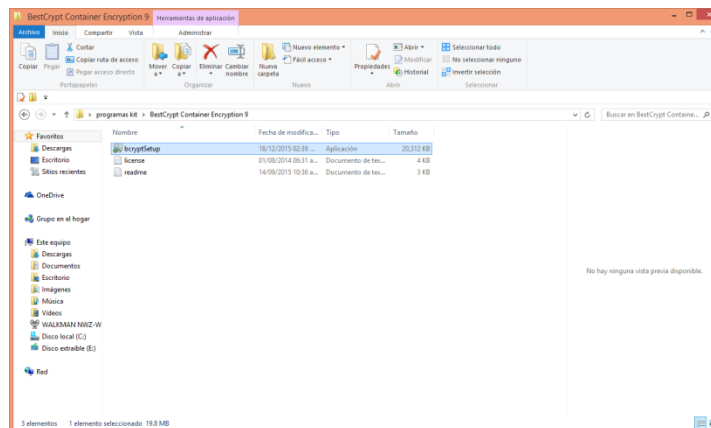


Figura 1. Instalador de BestCrypt Container Encryption.

1. Ejecutamos BestCrypt Container Encryption, ver figura 1.

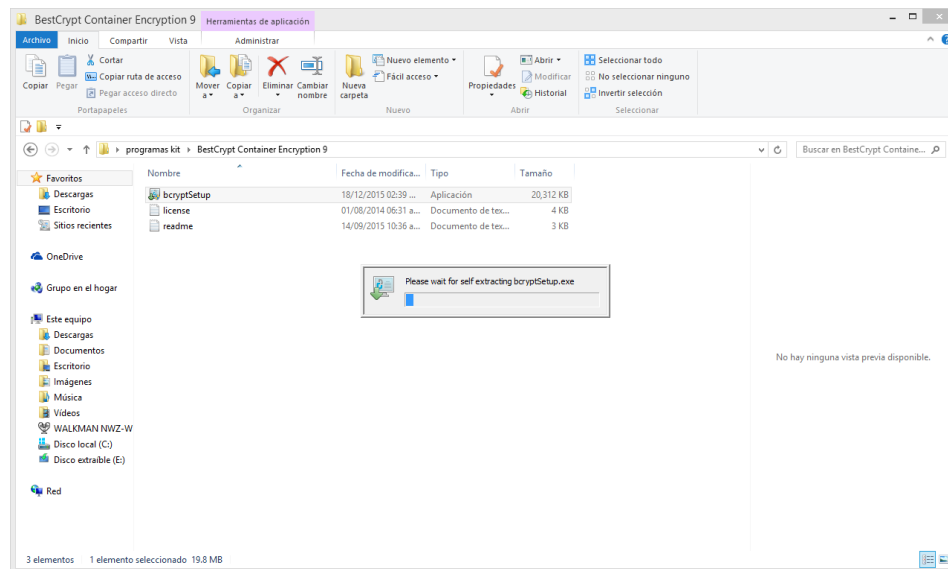


Figura 2. Instalando BestCrypt Container Encryption.

2. Se ejecutará el extractor del instalador, esperar hasta que termine de extraer ver figura 2.



Figura 3. Instalando BestCrypt Container Encryption.

3. Se ejecuta el cuadro siguiente, ver figura 3 damos clic en siguiente.

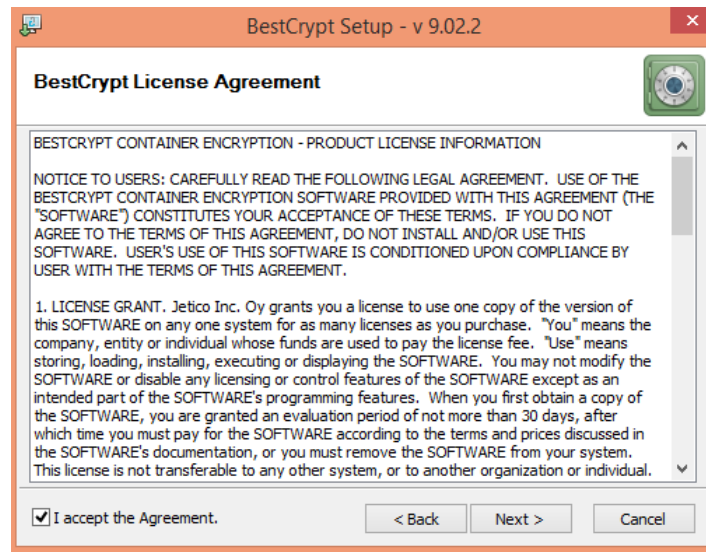


Figura 4. Instalando BestCrypt Container Encryption.

4. En el siguiente cuadro, ver figura 4, se aceptan los términos de licencia del software, y clic en next.

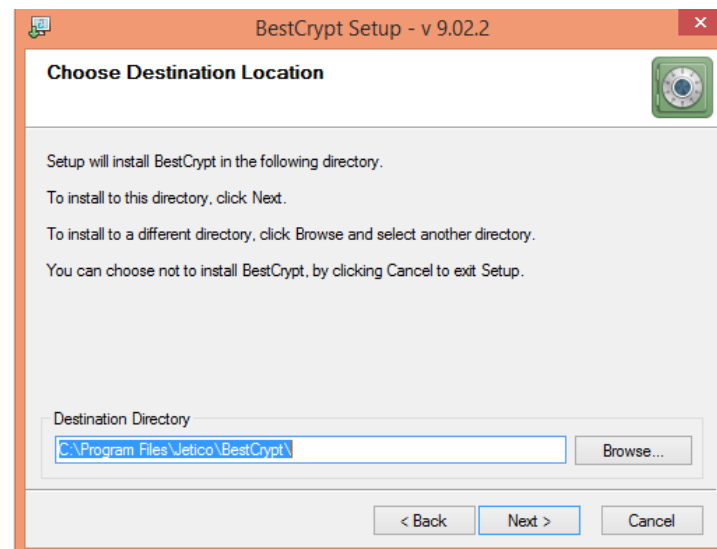


Figura 5. Instalando BestCrypt Container Encryption.

5. En el siguiente cuadro, ver figura 5, dar clic en next.

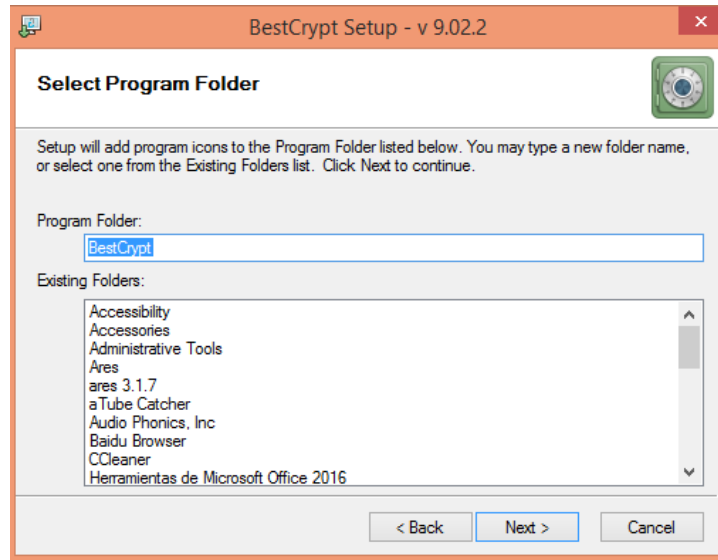


Figura 6. Instalando BestCrypt Container Encryption.

6. En el siguiente cuadro, ver figura 6, clic en next.

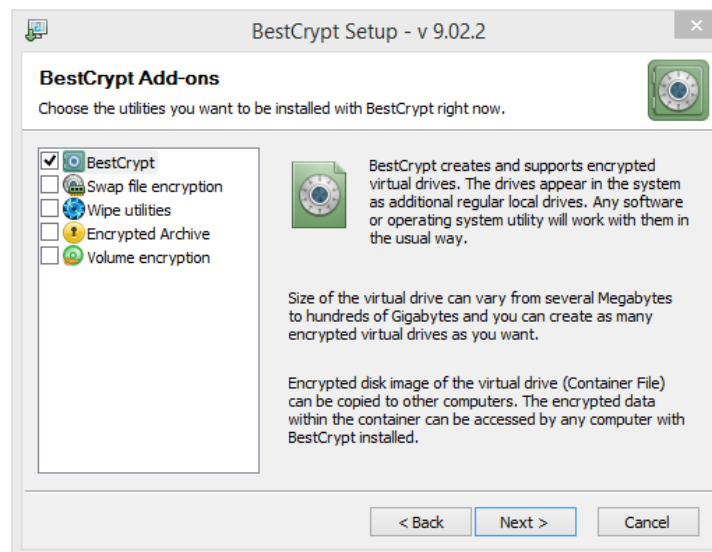


Figura 7. Instalando BestCrypt Container Encryption.

7. En el siguiente cuadro, ver figura 7 clic en next.

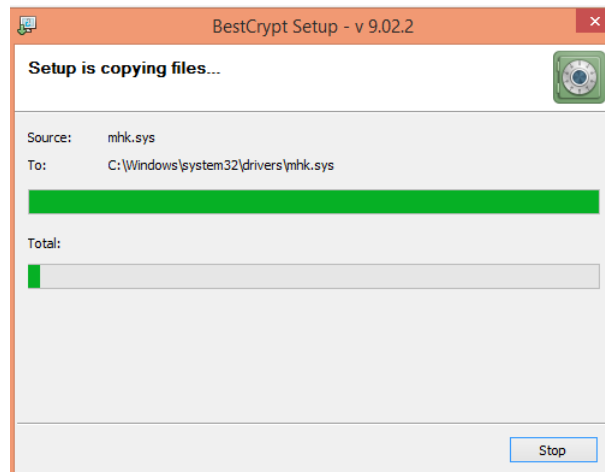


Figura 8. Instalando BestCrypt Container Encryption.

8. En el siguiente cuadro, ver figura 8. Esperar hasta que se instale el software.

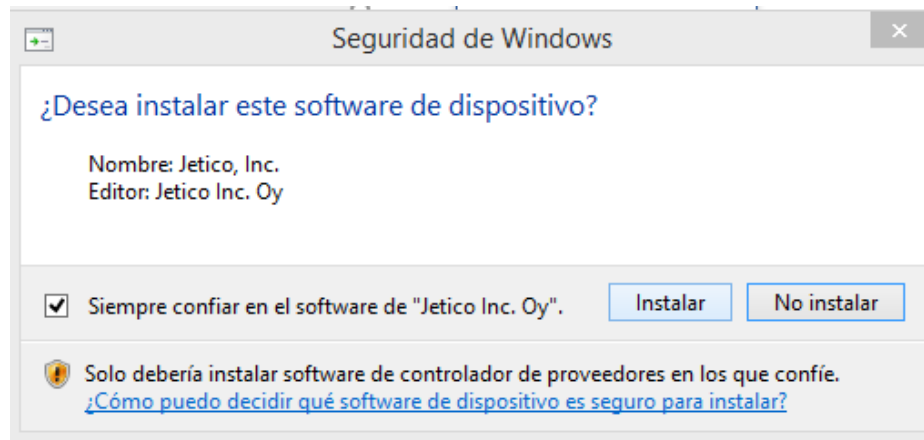


Figura 9. Instalando BestCrypt Container Encryption.

9. Se ejecuta un mensaje emergente, ver figura 9 clic en instalar.

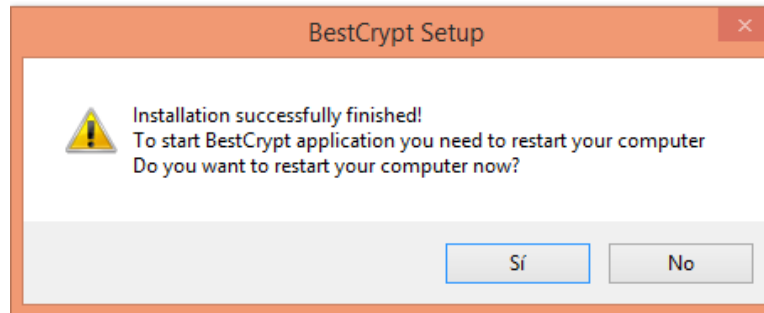


Figura 10. Instalando BestCrypt Container Encryption.

10. Al final saldrá un mensaje de reinicio del sistema, cerrar todo lo que se esté haciendo, clic en sí y se reiniciará. Quedará instalado el programa listo para utilizar.

Uso de BestCrypt Container Encryption.

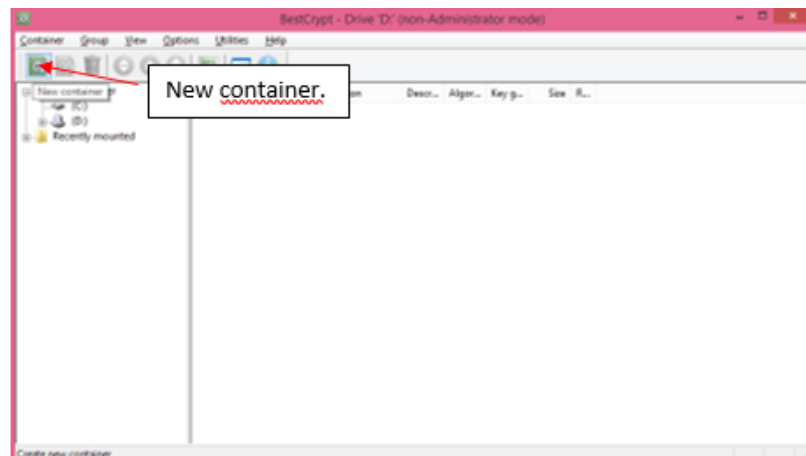


Figura 1. New container.

1. Clic en new container. Ver figura 1.

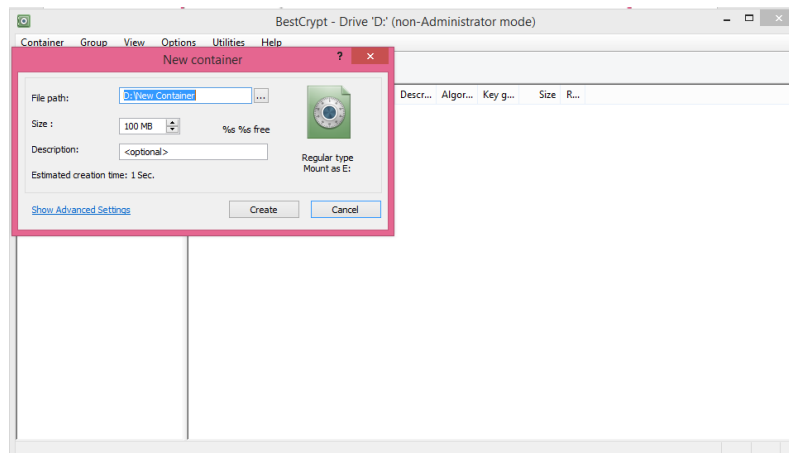


Figura 2. New container.

2. En el siguiente cuadro, ver figura 2 clic en créate.

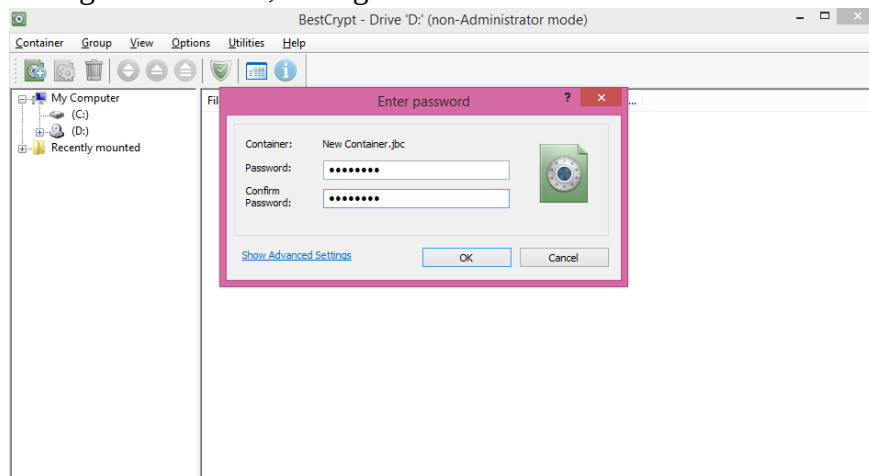


Figura 3. Ingresa contraseña.

3. En el siguiente cuadro ver figura 3 crear una contraseña dar clic en ok.

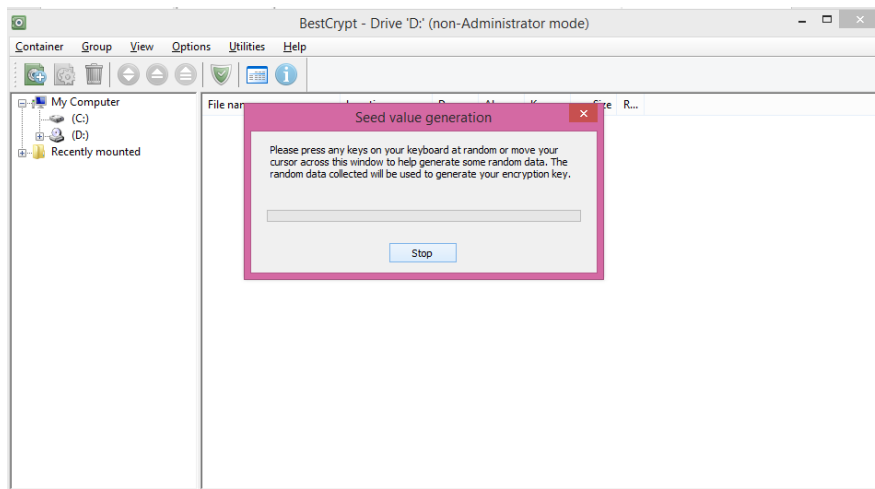


Figura 4. Cifrando.

4. Esperar hasta que cree el cifrado.

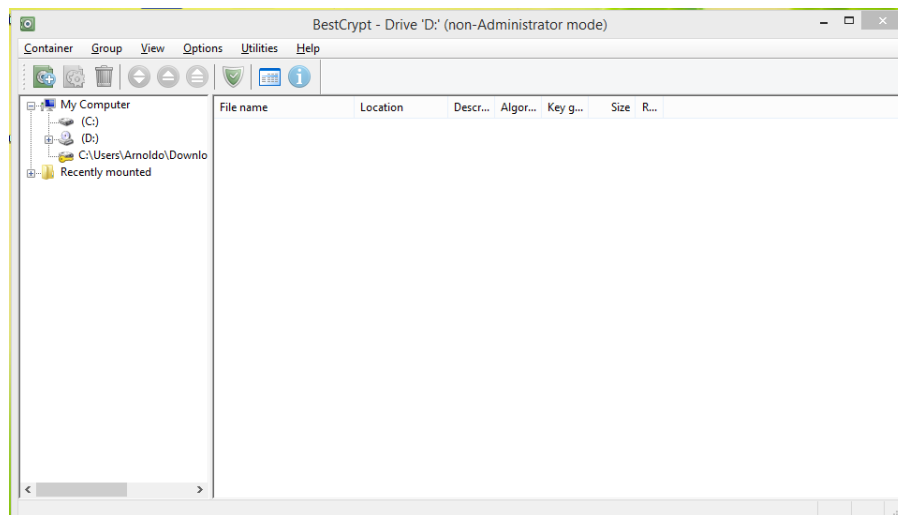


Figura 5. Encriptado.

5. Ver figura 5. Se habrá creado la unidad encriptado, donde se podrá guardar archivos videos, música entre otros.

2.1.12 descripción de DVD multimedia.

El DVD multimedia se realizará con el software Myautoplay, con el cual se creará la ventana principal del kit de seguridad informática y dentro de cada software tendrá el archivo instalador .exe o en el caso de los sistemas operativos Android el archivo APK, incluirá el manual de instalación y uso de cada software y la ficha técnica.

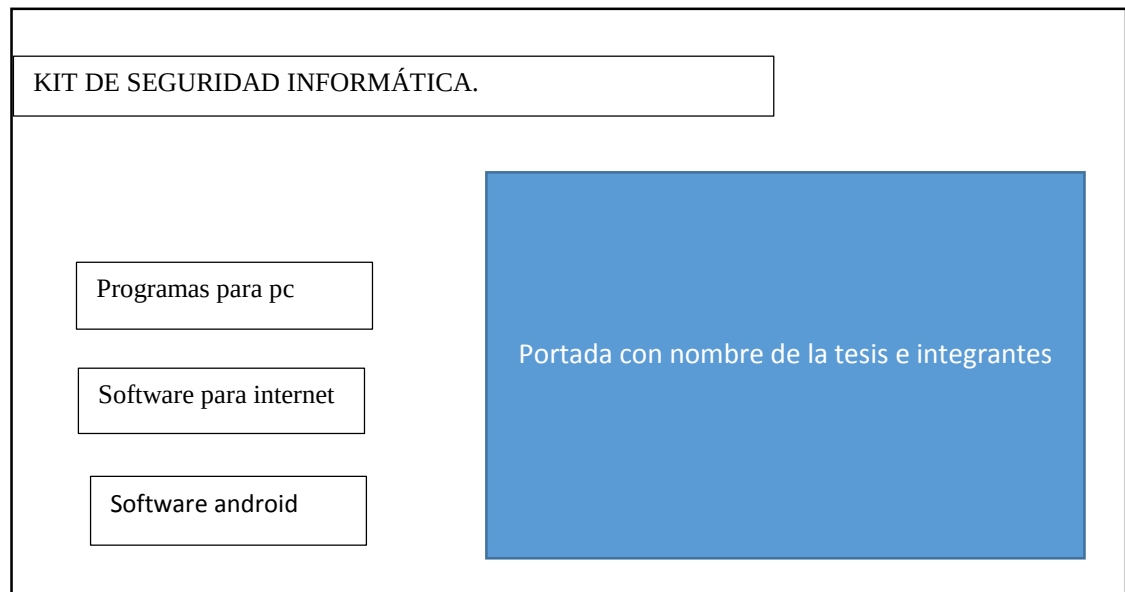


Figura 1, ventana principal del DVD multimedia

Dentro de cada software el contenido que se mostrara al dar clic en algún software en específico. A continuación, se muestra un modelo de cómo estará el contenido en cada software.

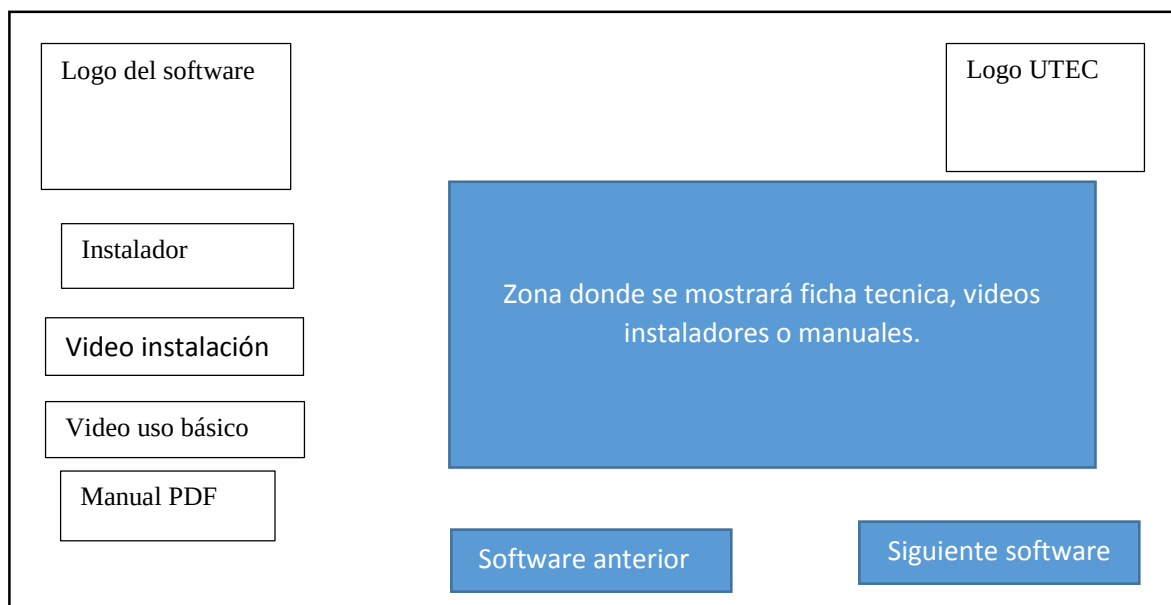


Figura 2, contenido de lo que contendrá cada software.

3.Marco teórico conceptual.

App Killers: (aplicaciones asesinas) es una aplicación que utiliza bastantes recursos de memoria RAM, se caracteriza porque reemplaza total o parcialmente a otros servicios tradicionales.

Anti-Rootkit: es una herramienta diseñada para detectar y eliminar las formas más sofisticadas y sigilosas de malware como rootkit.

APK: (Application Package File) es un paquete para el sistema operativo Android. Este formato es una variante del formato JAR de Java y se usa para distribuir e instalar componentes empaquetados para la plataforma Android para Smartphone y Tablet.

Bug: también conocidos como holes o agujeros. Defecto en un software o un hardware que no ha sido descubierto por los creadores o diseñadores de los mismos.

Botnet: es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática.¹ El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

Backdoor: en la informática, una puerta trasera (o en inglés backdoor) es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autenticación) para acceder al sistema. Aunque estas "puertas" pueden ser utilizadas para fines maliciosos y espionaje no siempre son un error, ya que pueden haber sido diseñadas con la intención de tener una entrada secreta.

Bloatware: (pronunciado: blout-uer) es como se le conoce a toda aplicación de poca utilidad y el cual consume innecesariamente espacio en disco o en memoria. Muchas de

estas aplicaciones vienen instaladas de fábrica por los fabricantes como una especie de subsidio para el precio del equipo.

Bucaneros: son los comerciantes de la red mas no existen en ella; aunque no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios. Su objetivo está centrado en comercializar o revender los productos que los Copyhackers les proporcionan, bajo un nuevo nombre comercial, con el ánimo de lucrarse en corto tiempo y con el más mínimo esfuerzo.

Copyhacker: son una nueva generación de falsificadores dedicados al crackeo de hardware, específicamente en el sector de tarjetas inteligentes.

Cracking: conducta delictiva en donde un individuo denominado cracker altera, modifica, elimina, borra los datos de un programa informático o de un documento con la finalidad de obtener un beneficio de dicha alteración; puede referirse a varias prácticas similares, o al conjunto de ellas:

Password cracking: quebrar la seguridad de una contraseña o password.

System cracking: quebrar la seguridad de un sistema informático.

Software cracking: quebrar la seguridad anticopia o antipiratería de un software.

Código malicioso: es código informático que provoca infracciones de seguridad para dañar un sistema informático. Se trata de un tipo de amenaza que no siempre puede bloquearse con un software antivirus por sí solo. El código malicioso incluye scripts de sitios web que pueden aprovechar vulnerabilidades con el fin de descargar malware.

Datos (informática): cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.

DDoS: es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

DSL: la línea de abonado digital o línea de suscripción digital, Digital Subscriber Line (DSL), es una familia de tecnologías que proporcionan el acceso a Internet mediante la transmisión de datos digitales a través de los cables de una red telefónica local.

Ethernet: es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD)

Exploit: (del inglés exploit, "explotar" o 'aprovechar') es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo

Hacker: cualquier persona que se dedica a hacer hacking. Debe ser bastante bueno con los ordenadores (como mínimo). Conocer bien el funcionamiento de los ordenadores y todo su relacionado. Muchas veces una vez que ha penetrado en un sistema suele dejar algún tipo de mensaje al administrador del mismo para que este sepa de la existencia de errores, Bugs o holes que permitieron el acceso.

HTTPS: Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de

aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

Hacking: el hacking es considerado un arte ya que busca la manera de atacar y buscar la vulnerabilidad de un sistema informático, un método de hacking diseñado por un hacker es compartido con otros.

Hardware: conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Ingeniería social: es una técnica por la cual se trata de convencer a alguien, por diversos medios (email, llamada telefónica, voz) para que nos proporcione información útil para poder ya sea acceder a instalaciones o poder acceder físicamente a un equipo informático.

Keylogger: es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Kernel o núcleo: se puede definir como el corazón de este sistema operativo. Es el encargado de que el software y el hardware de tu ordenador puedan trabajar juntos.

Lamer: principiante en el mundo del hacking que se las da de listo o que copia, descaradamente, el trabajo de otros hackers. Cuando se les descubre se les desprecia y se les expulsa del círculo en el que se han introducido.

LAN: una red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

Memoria RAM: memoria principal de la computadora, donde residen programas y datos, sobre la que se pueden efectuar operaciones de lectura y escritura.

Malware: código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Newbie: es el típico “cacharrero” de la red, sin proponérselo tropieza con una página Hacking y descubre que en ellas existen aéreas de descarga de buenos programas de Hackeo, baja todo y empieza a trabajar con ellos.

Open Handset Alliance (OHA): es una alianza comercial de 84 compañías que se dedica a desarrollar estándares abiertos para dispositivos móviles. Algunos de sus miembros son Google, HTC, Dell, Intel, Motorola, Qualcomm, Texas Instruments, Samsung, LG, T-Mobile, Nvidia y Wind River Systems.

Phishing o suplantación de identidad: es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito otra información bancaria

Pheaking: todo lo relacionado con el uso del teléfono o servicios telefónicos de forma gratuita. También incluye la modificación o intervención de las líneas telefónicas y las modificaciones de aparatos telefónicos con el fin de comunicarse gratuitamente.

Pirata informático: es un delincuente informático que se dedica a la copia y distribución de software ilegal. Este software puede ser comercial crackeado o

shareware registrado. También es otro nombre que reciben los crackers, no confundir con los hackers.

Rootkits: son formas ocultas de malware que los antivirus tradicionales normalmente no puedan detectar o eliminar.

Rogue AP: (también conocidos como Fake AP) es un punto de acceso que tiene por objetivo que los usuarios se conecten a él para, una vez dentro, capturar su tráfico y con ello, sus credenciales.

Rogue: se le denomina Rogue Software (o también Rogue Rogueware, FakeAVs, Badware, Scareware) a los “Falsos programas de seguridad” que no son realmente lo que dicen ser, sino que, todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado.

Software: conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Spyware o programa espía: es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Spam o correo basura: son los mensajes no solicitados, no deseados o de remitente desconocido y que son sumamente molestos

SIP: (Session Initiation Protocol.) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Fue desarrollado inicialmente en el grupo de trabajo IETF MMUSIC

(Multiparty Multimedia Session Control) y, a partir de septiembre de 1999, pasó al grupo de trabajo IETF SIP.

SSID: (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.

Spammer: persona o grupo dedicados a la distribución de correo electrónico no deseado, spam o spamdexing.

Teclado Virtual: es un elemento de la interfaz de usuario de un sistema que permite al usuario introducir caracteres en un dispositivo. En inglés es virtual keyboard. Un teclado virtual usualmente se ve en pantalla tal cual se vería un teclado real de computadora, pero con la posibilidad de teclear en este empleando los dedos (en una pantalla táctil), un ratón de computadora, un lápiz, etc.

Trashing: termino que podría traducirse como “recoger o buscar en la basura”. Se trata de buscar y encontrar en la basura (física o informática) datos que nos proporcionen información sensible de una empresa. Esos datos nos pueden dar acceso a cuentas bancarias, correos electrónicos importantes, reportes financieros, listas de usuarios y passwords, etc.

Ventana Emergente: (en inglés se le conoce como Pop-Up Windows) es una ventana de tu navegador de Internet que aparece automáticamente, sin ser solicitada y que usualmente tiene como finalidad desplegar publicidad, dirigir tráfico de Internet a ciertas páginas o recopilar direcciones de correo electrónico.

VPN: una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet

VoIP: es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP (Protocolo de Internet)

Widget: es una pequeña aplicación o programa, usualmente presentado en archivos o ficheros pequeños que son ejecutados por un motor de widgets o Widget Engine.

WEP: (Wired Equivalent Privacy, privacidad equivalente a conexión por cable) es una función opcional de IEEE 802.11 que se utiliza para proporcionar una seguridad a los datos que sea equivalente a la de los datos de una LAN conectada mediante cable sin técnicas de cifrado para mejora de la privacidad.

WPA2: (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA.

WPA: (Wi-Fi Protected Access) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP).

Warez: se refiere principalmente al material bajo copyright distribuido con infracción al derecho de autor.

Wannabe: programador experto que está a un paso de ser hacker. Todos los hackers han pasado por esta etapa y solo llegan a hacker cuando los veteranos deciden considerarlo uno de los suyos.

4.Documentación técnica.

DOCUMENTACIÓN TÉCNICA DE ADBLOCK PLUS.

¿Qué es Adblock Plus?

Adblock Plus es una extensión gratuita que permite entre otras cosas bloquear anuncios molestos, desactivar seguimiento y bloquear dominios conocidos para propagar malware. Disponible para Android, Chrome, Firefox, Internet Explorer, Maxthon, Opera, Safari y Yandex, Adblock plus utiliza filtros que desee bloquear todos los elementos no deseados.

¿Cómo funciona Adblock Plus?

Adblock Plus por sí mismo no tiene ninguna funcionalidad, bloquea agregando listas de filtros externos. Las listas de filtros son esencialmente un conjunto de reglas que le dicen a Adblock Plus cuales elementos de sitio web bloquear. Puede agregar cualquier lista de filtro que desee. Por ejemplo, bloqueo de seguimiento o Malware. También puede crear sus propias listas de filtros. Casi todos los filtros son de código abierto, por lo tanto, muchas listas de filtro han sido creadas por los usuarios de internet.

DATOS.

Autor: Creado por Wladimir Palant en 2006.

Licencia: Gratis

Idioma: inglés y español)

REQUISITOS.

Sistema Operativo: Microsoft Windows 7 o superior, Linux y MAC OS.

Compatible con los siguientes navegadores: Mozilla Firefox, Google Chrome, Opera, Android, Internet Explorer, Safari, Yandex, Maxthon, Microsoft Edge.

CARACTERÍSTICAS.

- ✓ Bloquea todo tipo de anuncios publicitarios en nuestra navegación.
- ✓ Desactiva el seguimiento y el historial realizado por ciertas páginas web para ofrecer publicidad personalizada.
- ✓ Bloquea el acceso a determinadas páginas potencialmente peligrosas.
- ✓ Consumo de memoria y CPU.
- ✓ Puede leer y crear filtros de archivos hosts.
- ✓ Es compatible con la mayoría de navegadores.

DOCUMENTACIÓN TÉCNICA DE BESTCRYPT CONTAINER ENCRYPTION.

BestCrypt Container Encryption previene fugas de datos no deseados mediante la protección de cualquier archivo seleccionado o carpetas en un equipo activo, estación de trabajo compartida o almacenamiento en red.

BestCrypt Container Encryption funciona en unidades virtuales intuitivamente fáciles con el uso transparente y acceso a los archivos. Y gracias a la compatibilidad en diferentes sistemas operativos, los archivos BestCrypt Container pueden ser movidos a cualquier equipo o medio de almacenamiento, trabajando sin problemas entre Windows, Mac OS y Linux.

BestCrypt Container Encryption Enterprise Edición incluye Jetico Central Manager para desplegar software cliente de forma remota a través de todas las estaciones de trabajo, controlar el uso de archivos contenedores cifrados y gestionar de forma centralizada

información de recuperación necesaria para acceder a los datos cifrados en caso de emergencia.

DATOS.

Autor: Jetico Inc. Oy.

Licencia: \$ 59.95.

Idioma: español e inglés.

REQUISITOS.

Sistema operativo: Windows, Linux y MAC OS.

CARACTERÍSTICAS.

- ✓ Selecciona almacena archivos carpetas en contenedores cifrados (unidades virtuales).
- ✓ Mover archivos contenedores BestCrypt entre cualquier medio de almacenamiento, a través de Windows Linux, y MAC OS.
- ✓ Versión para Windows incluye BC wipe normal.
- ✓ Cifra archivos de sistemas operativos de Windows.
- ✓ Encriptación de archivos y carpetas.
- ✓ Soporte de archivos previamente cifrados con la aplicación desfasada True Cryp.
- ✓ Protección archivos al subir a internet.
- ✓ Protege la vulnerabilidad de archivos.
- ✓ Tienda y acceso cifrado de archivos fácilmente vía unidades virtuales.
- ✓ Crear y administrar varios contenedores
- ✓ Monte unidad de cifrado como una subcarpeta

- ✓ Definir uso en entorno multiusuario
- ✓ Crear y acceso a contenedores al instante
- ✓ Trabajar con contenedores dinámicos
- ✓ Movimiento y tienda contenedores encriptados a través de sistemas Windows, Linux, Mac OS y Android.
- ✓ Desplegar, Monitor y recuperar contraseña con administración central
- ✓ Mejora de la seguridad
- ✓ Contenedores mejorados ocultos
- ✓ Operaciones con encabezados de contenedor
- ✓ Soporte para claves
- ✓ Soporte de anti-keylogger para el cifrado de clave pública
- ✓ Apoyo secreto compartir esquemas.

DOCUMENTACIÓN TÉCNICA DE HOTSPOT SHIELD.

Mejor conocido como VPN, la tecnología VPN permite enviar datos de cifrados a través de redes de antes no lo estuvieran. Además de ofrecer una navegación privada y segura por internet, las VPN como la de Hotspot Shield proporcionan una amplia gama de ventajas importantes. En comparación con un Proxy Web, la VPN también ofrece una seguridad y una privacidad en línea mucho mejores.

La VPN de Hotspot Shield es en la que confían más usuarios en el mundo, con más de 200 millones de descargas. Está disponible para sistemas operativos Mac OS, Windows y dispositivos: iPhone, iPad y Android.

DATOS.

Autor: AnchorFree Inc.

Licencia: Gratis y versión Hotspot Shield Elite de paga \$ 19.99 por 6 meses)

Idioma: español y varios idiomas.

REQUISITOS.

Sistema operativo: Windows, Androide, Linux y MAC OS

CARACTERÍSTICAS.

- ✓ Desbloquee sitios web como YouTube, Facebook, twitter u otros, ya sea en un centro educativo, en la biblioteca o en la oficina, con la VPN de Hotspot Shield. Evite los filtros y los cortafuegos establecidos por el administrador de red y acceda a su contenido favorito.
- ✓ Navegue de forma anónima: su seguridad y su privacidad son importantes, así que es posible que quiera navegar por Internet de forma anónima. La VPN gratuita de Hotspot Shield crea un túnel cifrado entre su equipo y nuestros servidores para permitirle realizar actividades en línea de forma anónima como, por ejemplo, visitar los sitios web que quiera, efectuar transacciones en línea o descargar archivos, sin que otros lo espíen o realicen un seguimiento de sus movimientos.
- ✓ Oculte su dirección IP: Internet está lleno de fisgones, de Spammers y de hackers. Monitorizan con total discreción sus actividades en línea y, cuando menos se lo espera, roban sus datos confidenciales, como la información de las tarjetas de crédito y las contraseñas. Al conectarse a Internet con Hotspot Shield

habilitado, obtiene una nueva dirección IP de EE. UU. Para enmascarar la real y poder navegar de forma anónima.

- ✓ Navegación privada y segura: la VPN ofrece un nivel mejorado de seguridad en línea. Si usa la VPN de Hotspot Shield para conectarse a Internet, podrá cifrar y proteger datos, contraseñas, transacciones financieras y mensajes instantáneos. Además, su información personal quedará fuera del alcance de los espías de la red.
- ✓ Seguridad de Wi-Fi: si navega por Internet en un punto de acceso Wi-Fi público, como el Starbucks de su localidad, cualquier usuario de dicha red podrá monitorizar y espiar lo que haga en la red. Independientemente de la ubicación desde la que se conecte, gracias a una VPN personal podrá proteger su sesión de navegación y mejorar considerablemente la privacidad de sus datos personales.
- ✓ Protección de malware: la VPN de Hotspot Shield le mostrará una alerta en el caso de que visite sitios que contengan Malware y, a continuación, los bloqueará. Detecta y bloquea más de 3,5 millones de sitios maliciosos y dedicados al fraude electrónico o al spam para que no infecten su dispositivo.

DOCUMENTACIÓN TÉCNICA DE FREE VPN PROXY BY BETTERNET ANDROID.

Free VPN - Betternet es una aplicación que permitirá acceder a cualquier página web del mundo sin restricciones de ningún tipo, evitando cualquier censura que haya en tu país. De la misma forma, se podrá acceder a servicios que normalmente estarían restringidos dentro de las fronteras.

DATOS.

Autor: Betternet Technologies Inc.

Licencia: gratis.

Idioma: español e inglés.

REQUISITOS.

Sistema Operativo: Android 4.0 o superior.

CARACTERÍSTICAS.

- ✓ Gratis para siempre.
- ✓ No requiere tarjetas de crédito.
- ✓ No se requiere registro ni inicio de sesión.
- ✓ No se guardan las sesiones de ningún usuario.
- ✓ Simple, conexión con un solo toque.
- ✓ Te conecta al servidor más rápido.
- ✓ Desbloquea webs y aplicaciones.
- ✓ Navegación anónima
- ✓ Protege la privacidad y asegura tu dispositivo

DOCUMENTACIÓN TÉCNICA ANDROID DEVICE MANAGER.

Android Device Manager puede geo localizar en el mapa los terminales Android asociados a tu cuenta Google. Y ofrece tres opciones: hacer sonar el celular, Tablet a todo volumen durante 5 minutos, bloquear el dispositivo o borrar todos los datos remotamente, muy útil para proteger tu privacidad.

Android Device Manager está en español, es gratis y recomendable para cualquier usuario de Android.

DATOS.

Autor: Google Inc.

Licencia: gratis.

Idioma: español e inglés.

REQUISITOS.

Sistema operativo: Android 4.0 o superior.

CARACTERÍSTICAS.

- ✓ Geolocalización en un mapa.
- ✓ Borrado de datos remoto.
- ✓ Funciona con todos tus dispositivos asociados.
- ✓ Útil en caso de robo o pérdida.
- ✓ Pierde su teléfono, usted aún podrá añadir una cerradura (o cambiar una cerradura existente) en su dispositivo.
- ✓ Protege su información personal y datos.

DOCUMENTACIÓN TÉCNICA CERRADURA (APP LOCK) ANDROID.

Con cerradura (AppLock) puede bloquear mensajes SMS, contactos, Gmail, Facebook, galería, Market, configuración, llamadas y cualquier aplicación que escojas, con abundantes opciones, protegiendo tu privacidad.

El funcionamiento de la aplicación es muy simple: el usuario tendrá que crear un patrón de desbloqueo asociado a la aplicación que quiera proteger, y a partir de ese momento

será necesario introducir dicho patrón para usar esa aplicación. Incluso si otro usuario intenta desinstalar esa aplicación, una ventana con el patrón de bloqueo se lo impedirá. Lo mejor de la aplicación es que podremos incluso esconder el icono de la misma, de manera que nadie sepa que la tenemos instalada y tan solo nosotros podremos verla escribiendo un código en el teclado numérico del teléfono.

Otra prestación interesante es la llamada bóveda de fotos, que nos permitirá mantener unas cuantas fotografías en una especie de caja fuerte que tan sólo nosotros podremos abrir.

Con esta utilidad podrás bloquear o desbloquear apps en función de la hora del día, es decir, que contarás con la posibilidad de asignar patrones que hagan que una aplicación se bloquee por las mañanas y sea accesible por las noches, siempre en función del uso que hagas de ella y el momento y el lugar. En este sentido, podrás crear diferentes perfiles que activar o desactivar en un momento concreto. Por ejemplo, activa tu perfil de trabajo cuando estés en la oficina y no quieras que ningún compañero cotillee herramientas determinadas, o activa el perfil casa si lo que quieres es más libertad.

DATOS.

Autor: DoMobile Ltd

Licencia: gratis.

Idioma: español.

REQUISITOS.

Sistema operativo: Android 4.0 o superior.

CARACTERÍSTICAS.

- ✓ Protege cualquier aplicación usando contraseña o patrón.
- ✓ Bóveda de fotos
- ✓ Bóveda de video
- ✓ Personalizar fondo, seleccionar foto favorita
- ✓ Perfiles, modificar bloqueos con facilidad
- ✓ Bloqueo automático después de cierto tiempo
- ✓ Bloqueo automático en cierta posición
- ✓ Ocultar ícono de AppLock
- ✓ Teclado aleatorio
- ✓ Interruptor de bloqueo (Wi-Fi, BT, Datos 3G/4G.)
- ✓ Widget para bloqueo/desbloqueo rápido.
- ✓ Bloquea llamadas entrantes o salientes.
- ✓ Bloquea la configuración del sistema.
- ✓ Bloquea los servicios de Google Play Store.
- ✓ Cambio rápido del bloqueo en la barra de notificaciones.
- ✓ Política de Re-bloqueo: Permite salida rápida, no hay necesidad de volver a bloquear.
- ✓ Previene la desinstalación de aplicaciones.
- ✓ Esconde el ícono de AppLock del menú de aplicaciones.
- ✓ Puedes prevenir la desinstalación de AppLock.
- ✓ AppLock no puede ser detenida por gestores de tareas (app killers).
- ✓ Poco uso de memoria y ahorra batería.

DOCUMENTACIÓN TÉCNICA DE AVG ANTIVIRUS FREE.

AVG Anti-Virus Free Edition es un antivirus de primer nivel. Su motor se encuentra entre los más afamados del sector, a la misma altura que el de Avast o el de Avira. Las diferentes herramientas que ofrece son capaces de proteger tu PC de todo tipo de amenazas, mientras que su bajo consumo de recursos y su excelente velocidad de análisis lo vuelven un candidato ideal para quienes no poseen un ordenador de última generación. Diferencias con la versión de pago y con Internet Security.

A diferencia de esta versión gratuita, la versión de pago de AVG Anti-Virus incluye las funciones online Shield, que te protege de descargas potencialmente peligrosas, y Data Safe, que encripta con contraseña tus archivos personales. Internet Security, además de las prestaciones anteriores, te ofrece un cortafuego y un filtro anti-spam para tu correo electrónico.

DATOS

Autor: AVG Technologies CZ, s.r.o.

Licencia: gratis

Idioma: español.

Versiones:

REQUISITOS

Sistema operativo: Windows 7 o superior, MAC OS y Android.

CARACTERÍSTICAS

- ✓ Bloquea virus, spyware y otros malware.
- ✓ Cubre todos los dispositivos desde un sencillo panel.

- ✓ Bloquea a los hackers para poder realizar compras y operaciones bancarias con más seguridad.
- ✓ Protección de Vínculos Analiza vínculos de la web, Twitter y Facebook.
- ✓ Provee actualizaciones de seguridad en tiempo real.
- ✓ Mantenga su bandeja de entrada libre de spam y estafas.
- ✓ Mejorada la detección de malware.
- ✓ es uno de los mejores antivirus del mercado. Es muy potente, presenta una interfaz bien diseñada y dispone de una amplia variedad de funciones.
- ✓ es un poderoso antivirus que te protege de virus, gusanos, troyanos, spyware y rootkits mientras navegas por la red o revisas tu correo electrónico.
- ✓ protege tu privacidad y evita el robo de tus datos: es capaz de analizar el comportamiento de todos los programas instalados y de bloquear las actividades sospechosas.
- ✓ te permite programar los análisis de tu PC y también puedes elegir entre revisar todo tu sistema o sólo una parte del mismo. Además, es posible ejecutar un análisis específico para detectar rootkits.
- ✓ también incluye un verificador de enlaces, Link-Scanner, el cual analiza la confiabilidad de las páginas web que visitas, así como de los enlaces publicados en Twitter, Facebook y en otras redes sociales.

DOCUMENTACIÓN TÉCNICA MALWAREBYTES.

Malwarebytes Anti-Malware líder en la industria anti-malware y anti-spyware scanner detecta y elimina malware como gusanos, troyanos, rogues, spyware, bots y más. Tecnología anti-rootkits perfora hacia abajo y elimina los rootkits profundamente enraizadas, una de las formas más peligrosas de malware. Si tienes malware en su computadora, Malwarebytes Anti-Malware lo destruirá. Restaurar el equipo a su antigua gloria.

DATOS

Autor: Malwarebytes

Licencia: free y Premium \$ 24.95 por un año.

Idioma: español.

Sistema operativo: Windows 7 o superior, MAC OS y Android.

CARACTERÍSTICAS

Limpia las infecciones.

- ✓ Fácil de respirar. Búsqueda automática funciona para usted, para que nunca tenga que preocuparse de contraer la infección. Ordenador y sus datos se mantiene seguro.
- ✓ Detecta y elimina malwares en su versión gratuita.
- ✓ Protege frente a posibles infecciones (versión de pago)
- ✓ Soporte para Windows XP, Vista, 7, 8 y 10 (32-bit y 64-bit).
- ✓ Malwarebytes Anti-Rootkit integrado en el escáner
- ✓ Tecnología de exploración y detección heurística avanzada.
- ✓ 100% compatible con los principales antivirus.

DOCUMENTACIÓN TÉCNICA DE COMODO FIREWALL

Cómodo firewall te permite asegurar tu sistema contra ataques de todo tipo, como virus, troyanos, ataques de hackers o cualquier otro tipo de software malintencionado que haya podido entrar en tu pc, podrás controlar al detalle las aplicaciones que tienen acceso a Internet, crear reglas determinadas para algunas de ellas, monitorizar el tráfico de tu conexión en tiempo real para detectar posibles cuellos de botella y mucho más, te mostrará alertas de todos los intentos de conexión establecidos con tu máquina (tanto de entrada como de salida), lo que te permitirá vigilar todas las aplicaciones y detectar usos fraudulentos o no esperados de la red.

Cómodo firewall es un cortafuego (firewall) completo y renombrado, es gratuito para uso personal. Este te ayuda a proteger tu computadora de conexiones no autorizadas hacia y desde internet. Este capítulo está diseñado para satisfacer las necesidades tanto de usuarios principiantes como de avanzados.

DATOS

Autor: Comodo Group, Inc.

Licencia: gratis

Idioma: español e inglés.

REQUISITOS

Sistema operativo: Windows vista, 7, 8,8.1 y 10

CARACTERÍSTICAS

- ✓ Completa protección contra troyanos, root kits, spyware y hackers

- ✓ Utilidad malware Scan, que comprueba el sistema en busca de virus antes de instalar el programa
- ✓ Dos modos de instalación, uno básico con una configuración mínima, y otra avanzada donde se puede configurar muchas opciones para personas con más experiencia
- ✓ Con el módulo Defense mas, te ofrece protección contra root kits, inyección de código malicioso en procesos del sistema, monitoreo de ejecución de programas y ejecutables antes de que estos se carguen en memoria, te alerta cuando un programa desconocido intenta ser instalado, y previene que algún virus intente modificar archivos esenciales del sistema operativo sin nuestro consentimiento
- ✓ Un pequeño bloqueador de ventanas pop up.
- ✓ Tiene una interfaz de programa amigable, y contiene asistentes que facilitan el proceso de configuración.
- ✓ Soporte de actualizaciones automáticas, que se pueden configurar en el inicio del sistema o en forma manual para estar al día y bien seguro.

5.Presupuesto.

Presupuesto.

Horas hombre (elaboración de material, instalación, actualización y mantenimiento de productos)	\$ 300.00
Alquiler de material multimedia (cañón, laptops, etc.)	\$ 50.00
Fotocopias e impresiones (cada manual)	\$ 40.00
Viajes	\$ 50.00
Otros gastos	\$ 30.00
Total + softwares gratuitos	\$ 470.00

Con Software de Paga.

BestCrypt Container Encryption	\$ 59.95
Hotspot Shield Elite.	\$ 19.99 (6 meses)
AVG Antivirus 1 pc	\$ 39.99 1 año
MalwareBytes Premium 1 pc	\$ 24.95 1 año
Total	\$ 144.88
Total, Presupuesto + software de paga	\$ 614.88

Nota: algunos precios de presupuesto y software de paga pueden variar.

Capítulo III

Desarrollo de la solución.

1.Propuesta de la solución.

Con el desarrollo de este proyecto se brindará una herramienta tecnológica a los laboratorios de la Universidad Tecnológica de El Salvador, para la protección de los datos digitales que los estudiantes manipulan en los centros de cómputos de la Universidad, también se espera que sirva como medio de información e investigación en los softwares que existen para proteger en la seguridad de computadoras, como también seguridad en internet y seguridad en dispositivos Android. Para protegerse de visitar páginas de internet con contenidos de Malware, fraudes informáticos y otros delitos informáticos que se pueden cometer por medio de los dispositivos electrónicos, algunas veces los estudiantes dejan expuestos sus cuentas personales(Facebook, Twitter, Portal UTEC, Aula Virtual , cuentas de Google, etc.) y en algunas ocasiones pueden estar expuestos a que les roben sus datos personales poniendo en peligro su privacidad, direcciones de casa, contactos correo o números de tarjetas de crédito. Además, como hoy en día, la mayor parte de los estudiantes, la información que ingresan a internet, además de utilizar computadoras utilizan los Smartphone el cual es el medio más común que utilizan para realizar sus tareas diarias como comunicarse con otros estudiantes, enviar o revisar los correos electrónicos o simplemente visitar las redes sociales, es fundamental la seguridad ya que la mayoría de estudiantes poseen un dispositivo Android. Por ello nace nuestro tema de investigación desarrollo de un kit de

seguridad informática enfocada para la protección de la información digital tanto en Hardware como en Software para la Universidad Tecnológica de El Salvador.

Con la elaboración de este proyecto se ayudará a reforzar las competencias de los estudiantes en la Universidad Tecnológica de El Salvador siendo un material de apoyo para que conozcan sobre la seguridad informática y los diferentes programas que existen tanto en seguridad de PC, seguridad en internet, seguridad en Android, que permita mejorar la competitividad que los estudiantes necesitan mejorar en torno a la seguridad informática.

Para ello se diseñó un kit de seguridad informática en un DVD multimedia el cual contendrá programas para la seguridad informática Tanto en seguridad en PC, seguridad en internet, y seguridad en dispositivos Android, como también contendrá para cada programa su respectivo manual de instalación y uso, una ficha técnica de cada programa, siendo todos estos productos un material de apoyo extra para la Universidad Tecnológica de El Salvador para el beneficio de los estudiantes.

Para seleccionar las herramientas de software que se incluyeron en el DVD multimedia se realizó un proceso para identificar las herramientas más básicas utilizando un total de 3 softwares por cada área 3 en seguridad pc, 3 en seguridad internet, 3 en seguridad Android. Luego de seleccionar los programas se seleccionó por medio de una evaluación técnica y económica los mejores programas, seleccionando un total de 9, que son los elegidos en factibilidad técnica ya que cumplían mejor con las características evaluadas cumpliendo con el 95% de calificación requerida, por lo que el DVD multimedia cuenta

con 9 programas de seguridad las cuales están distribuidas de la siguiente manera: 3 softwares de seguridad PC, 3 softwares de seguridad internet y 3 softwares de seguridad en Android.

Se sabe que una computadora existen muchas áreas que proteger, pero porque se eligieron 3 softwares y no más, se eligieron 3 softwares ya que con esto se estaba evitando sobrecargar los recursos con las que cuenta un computador, entre los softwares para protección de PC se eligió:

- ✓ Avg Antivirus.
- ✓ Comodo Firewall.
- ✓ Bestcrypt Container Encryption,

Otra de las áreas en las cuales enfocamos la protección fue la de internet, se sabe que la protección de internet puede ser muy extensa y difícil, aunque no existe protección 100% segura se tratará de reducir los riesgos que se podrían encontrar cuando se navega por internet. Entre los softwares para la navegación por internet que se incluyeron fueron.

- ✓ HotSpot Shield
- ✓ Malwarebytes
- ✓ Adblock Plus.

Además de la protección en las computadoras e internet, otro dispositivo más usado por los estudiantes y en la cual se podría decir también que se maneja un flujo constante de información es el Smartphone en este caso se enfocó la protección a dispositivos que utilizan el sistema operativo Android ya que en El Salvador, aparte del iPhone con el sistema operativo IOS, el Android es el más utilizado por los estudiantes de la

Universidad Tecnológica de El Salvador ya que cuenta con una amplia gama de aplicaciones entre gratuitas y de paga. En este caso también se utilizó 3 aplicaciones de seguridad, para evitar sobre cargar el dispositivo y no ralentizar las demás aplicaciones con las que cuentan los usuarios.

Las aplicaciones que se utilizaron fueron gratuitas, pero para una mejor protección se recomienda al usuario utilizar una de pago.

- ✓ AppLock (Cerradura)
- ✓ Android Device Manager
- ✓ Free VPN.

El presente DVD multimedia se realizó para la Universidad Tecnológica de El salvador para fortalecer en los estudiantes el conocimiento sobre el tema de seguridad informática creando una herramienta de mucha utilidad para seguridad en internet, PC y dispositivos Android.

1.1. producto 1, manual de instalación y uso.

El manual se realiza con el propósito de guiar a cada uno de los estudiantes en lo que es la correcta instalación y activación de cada programa, así como también de orientar en el uso correcto del mismo.

El manual de instalación y uso esta creado en Microsoft Office Word 2016 en página tamaño carta enumeradas y con su respectivo índice con márgenes superior izquierdo de 4.0 CM e inferior derecho de 2.5 CM a doble espacio, cuenta con una portada al inicio diseñada con imágenes de algunos de los programas que conforman el DVD multimedia,

con título la letra en general es de 12 tipo Times New Román y los títulos 16 negrita, cuenta con una introducción.

Detalla de forma instructiva paso a paso, y con captura de imágenes del proceso de instalación y uso, están enumeradas y con título, cada una para hacer más fácil la comprensión por el lector, el manual de instalación y uso consta de 77 páginas orientadas al uso correcto de los programas que componen el DVD multimedia

La implementación de este manual de instalación y uso se lleva a cabo cuando el usuario necesita hacer uso de un programa específico del kit de seguridad informática por ejemplo el usuario necesita protección para sus pc puede dirigirse al manual y buscar un programa antivirus y verificar los pasos e instrucciones de instalación y uso en el apartado de protección para pc.

1.2. producto 2, fichas técnicas.

El tercer producto es el diseño de fichas técnicas de cada programa Las fichas técnicas se realizaron con el propósito de servir como un segundo material de apoyo extra, para los alumnos de La Universidad Tecnológica de El Salvador, ya que dentro de ellas se encuentran plasmadas cada una de las características propias de cada uno de los programas que conforman el kit de seguridad informática multimedia.

La ficha técnica cuenta con una portada al inicio, elaborada con imágenes de los programas utilizados en el DVD multimedia, con un borde solo la portada inicial, un título, letra estilo Times New Román en general. El primer título tamaño 16 y segundos títulos tamaño 13 tamaño de letra en general 10

Cuenta con una introducción a la ficha técnica, además cuenta con un índice automático para hacer del lector una búsqueda más rápida de la información que quiera, siendo del documento más óptimo y preciso para el lector.

La ficha técnica se elaborará en páginas de papel bond tamaño carta con márgenes superior izquierdo de 4.0 CM. E inferior derecho de 2.5 CM. Está compuesto por una tabla por cada programa cada tabla esta enumerada y con título al programa que pertenece.

El documento de las fichas técnicas está compuesto por un total 8 paginas el cual se menciona cada una de las características principales de cada uno de los programas que se incluyen en el kit de seguridad informática multimedia, así como también se incluyen los requisitos mínimos del sistema para su correcta instalación y funcionamiento, estas fichas tienen como objetivo orientar a los estudiantes a seleccionar adecuadamente los programas en base a las características que se necesitan y la capacidad de consumo que se necesitan a la hora de su debido uso.

La implementación de estas fichas técnicas se lleva a cabo cuando el usuario necesita hacer uso de un programa específico del kit de seguridad informática multimedia, por ejemplo, el usuario necesita usar un programa para protección del internet, pero necesita saber las características del programa para ver cuál es el que más le conviene utilizar y también para poder ver cuáles son los requisitos mínimos del sistema para proceder con la instalación y su respectivo uso.

1.3. producto 3, DVD multimedia.

El contenido del DVD multimedia consta de 9 programas de seguridad informática el cual fue clasificado en 3 partes, es decir, se investigaron 3 softwares para protección en computadoras, 3 softwares para internet y 3 softwares para dispositivos con sistema operativo Android.

En la ventana principal, en la barra de título contara con el nombre y logo de la Universidad Tecnológica de El Salvador.

Seguido dentro de la ventana principal estará el nombre DVD multimedia “Kit de seguridad informática”, abajo del nombre de DVD multimedia estarán los programas ya clasificados en grupo, además estará la portada con el nombre la Universidad el tema y los estudiantes del proyecto.

- ✓ Programas para PC.
- ✓ Programas Para Internet
- ✓ Programas para Android.

A continuación, se mostrará un breve ejemplo de cómo estará construida la página principal del DVD multimedia.



Figura 1, ventana principal

Al dar clic en cualquier grupo de software se abrirá otra ventana, donde, al inicio se mostrará el logo del software al que se está instalando, además que mostrará la ficha técnica que tendrá los requerimientos para la instalación de dicho programa. Seguido estarán un grupo de cuatro botones, los cuales son:

Instalar: se mostrará el instalador del programa.

Video instalación: un video que mostrara como instalar dicho software.

Video uso básico: un video breve de cómo se utiliza dicho programa.

Manual: un manual en formato PDF que tendrá imagen del software, índice e introducción y los pasos de instalación y uso del software que se refiera.

Para avanzar a los demás softwares del mismo grupo, estará el botón “siguiente software” el cual redireccionará al siguiente software el cual contendrá los mismos botones que la pagina anterior, además está incluido un botón de inicio para poder regresar a la página principal del DVD multimedia.



Figura 2, ventana de ficha técnica.

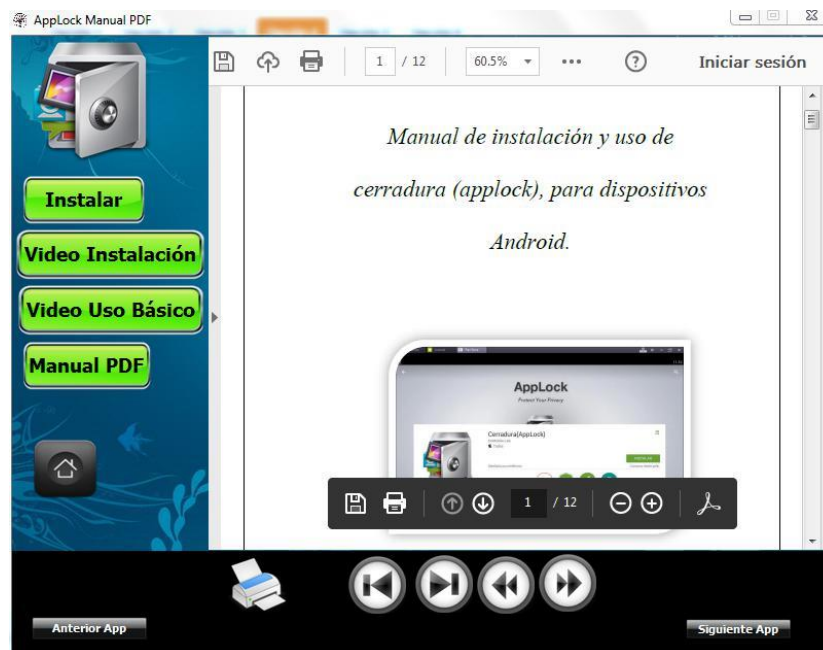


figura 3, ventana manual PDF.

En los grupos de programas para Android estará el APK disponible, el cual se tendrá que copiar al dispositivo donde se requiera la instalación, también estará un link que redireccionará a la página de GooglePlay donde se podrá instalar desde internet previa conexión con alguna red Wifi disponible.

También como producto agregado a los softwares de PC, Internet y Android, se han incluido algunos softwares, con lo cual beneficiará a los estudiantes y a la Universidad Tecnológica de El Salvador. Los softwares fueron puestos en un grupo en el DVD multimedia el cual lleva como nombre + Redes Sociales.

Nota: Para la instalación con el APK con cualquier dispositivo Android hay que activar la casilla “orígenes desconocidos” la cual se activa desde la ruta: Configuración-seguridad.

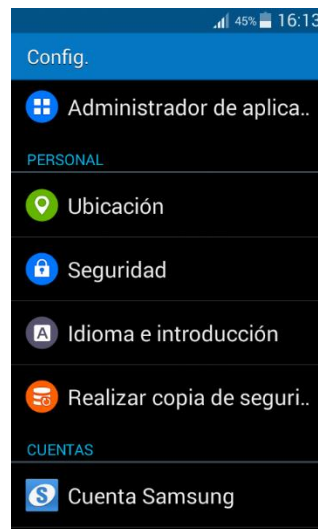


Figura 1, Configuración.

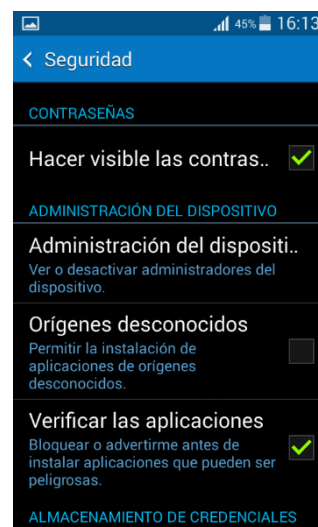


Figura 2, Seguridad.

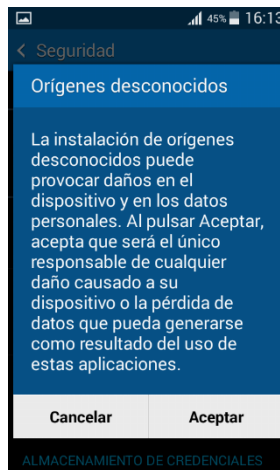


Figura 3, Aceptar.

Seguido dar en aceptar para poder instalar el APK en el dispositivo.

2.Conclusiones.

- Al concluir este proyecto se ayudará a que los estudiantes de la Universidad Tecnológica de El Salvador tengan un conocimiento sobre seguridad informática y disminuir el robo de información personal.
- Esta información será de utilidad para los laboratorios de la Universidad Tecnológica de El Salvador, una herramienta que podrán utilizar en la prevención del robo de datos personales de los estudiantes.
- La investigación realizada sobre los softwares de seguridad informática ayudará al usuario a disminuir el riesgo de robo de información, especialmente en los dispositivos Android que son los más vulnerables en la república de El Salvador.
- En la actualidad las tecnologías avanzan rápidamente por lo que la seguridad informática es muy importante, y por lo cual se debe estar muy informado para evitar ser víctima de robos informáticos.

- El tema de seguridad informática en los laboratorios es muy importante ya que se pueden reducir los daños que pudieran causar algún virus o ejecutar un programa malicioso que contenga algún malware, virus troyano o gusano.
- Los productos desarrollados con este proyecto ayudarán a transmitir un poco de conocimiento sobre seguridad informática y también ayudará a los estudiantes a poder disminuir el riesgo de robo de su información personal.

3.Recomendaciones.

- Para obtener mejores resultados para la seguridad informática de los datos se recomienda actualizar los programas en su versión de paga para obtener todas las herramientas y características que no poseen las versiones free.
- Para el usuario, mantener en constante actualización los drivers, sistema operativo, antivirus y demás programas de seguridad.
- En cuanto a seguridad en hardware es recomendable tener siempre un regulador de voltaje o UPS conectado a una computadora así se evitaría el daño físico de los dispositivos de hardware por un corto circuito y se evitaría la pérdida de información.
- Tener una copia de seguridad de la información tanto en las computadoras como en los dispositivos Android.
- Para los usuarios de dispositivos Android se recomienda evitar las descargas de Apps de terceros o de sitios desconocidos, siempre descargarlas, en el caso de los Android de GooglePlay o de páginas oficiales de los desarrolladores de las Apps.

- Hacer buen uso del kit de seguridad informática y utilizar los softwares que contienen crack o parche solo para fines educativos.
- En cuanto a los dispositivos Android se recomienda al usuario no instalar más de 3 Apps de seguridad ya que algunos de estos trabajan en tiempo real y podría ralentizar el dispositivo.
- Para extender el tiempo de uso de los dispositivos de hardware mantenerlo fuera del alcance de la humedad o de sitios cercanos a la humedad.
- También es recomendable mantener los dispositivos de hardware limpios ya que el polvo acumulado por largos periodos de tiempo pueda ocasionar daños a los circuitos de los dispositivos.
- Muy importante mantener ventilados los dispositivos de hardware que generen demasiado calor para evitar daños por sobrecalentamiento.
- Hacer las compras de licencias de paga de los softwares en las páginas web oficiales de los desarrolladores.
- Ampliar el tema en software de recuperación de información.
- Es recomendable ampliar más el tema de dispositivos Android.

4.Referencias

- Alegsa, L. (2010). *Definición de manual de usuario*. Recuperado de <http://www.alegsa.com.ar/Dic/manual%20de%20usuario.php>
- Alegsa, L. (2010). *Definición de virus (informático)*. Recuperado de <http://www.alegsa.com.ar/Dic/virus.php>
- Alerta en línea. (2011). *Phishing*. Recuperado de <https://www.alertaenlinea.gov/articulos/s0003-phishing>
- Android. (2016). *Android*. Recuperado de https://www.android.com/intl/es-419_mx/
- Asamblea Legislativa de El Salvador. (2016). *Ley especial contra los delitos informáticos y conexos*. Recuperado de <http://www.asamblea.gob.sv/eparlamento/indicelegislativo/buscador-de-documentos-legislativos/ley-especial-contra-los-delitos-informaticos-y-conexos>
- Asamblea Legislativa de El Salvador. (2016). *Ley de delitos informaticos regulará conductas delictivas mediante uso de las TIC*. Recuperado de <http://www.asamblea.gob.sv/noticias/archivo-de-noticias/ley-de-delitos-informaticos-regulara-conductas-delictivas-mediante-uso-de-las-tic/?searchterm=ley%20contra%20delitos%20informaticos>
- Asamblea Legislativa de El Salvador. (2014). *Ley especial contra actos de terrorismo*. Recuperado de <http://www.asamblea.gob.sv/eparlamento/indicelegislativo/buscador-de-documentos-legislativos/ley-especial-contra-actos-de-terrorismo>
- Ávila Mejía, Ó. (2011). *Android*. Recuperado de <http://www.izt.uam.mx/newpage/contactos/revista/83/pdfs/android.pdf>

- Callejas López, J. E. & Vásquez Cartegena, D. E. (2015). *Elaboración de un kit de software de informática forense para su uso en el área de seguridad y recuperación de informacion en beneficio de los laboratorios de informatica de la Universidad Tecnológica de El Salvador* (Tesis de ingeniería). Universidad Tecnológica de El Salvador, San Salvador, SV. Recuperado de <http://biblioteca.utec.edu.sv/siab/virtual/tesis/88763.pdf>
- Definicion. (2016). *Definición de seguridad informática*. Recuperado de <http://definicion.de/seguridad-informatica/>
- DefinicionABC. (2016). *Definición de seguridad informática*. Recuperado de <http://www.definicionabc.com/tecnologia/seguridad-informatica.php>
- El país. (2007). *Cómo combatir el Spam*. Recuperado de http://elpais.com/diario/2007/05/10/ciberpais/1178761885_850215.html
- Erb, M. (2008). *Gestión de Riesgo en la Seguridad Informática*. Recuperado de https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/
- Ferri-Benedetti, F. (2010). *Botnets: cómo evitar que tu PC se convierta en un zombi*. Recuperado de <http://articulos.softonic.com/botnets-ddos-wikileaks-virus>
- García Solis, S. E.; Hernández Osegueda, R. A. & Orellana Lopez, E. M. (2009). *Implementación, diseño y desarrollo de un material de contenido teórico de informática forense como referencia del material extracurricular aplicada a la materia de software de mantenimiento para los estudiantes de la carrera de técnico ingeniería de hardware*. (Tesis inédita de ingeniería), Universidad Tecnológica de El Salvador, San Salvador, SV.

- Gómez Labrador, R. M. (2005). *Tipos de licencias de software*. Recuperado de <http://www.informatica.us.es/~ramon/articulos/LicenciasSoftware.pdf>
- González Morales, A. (2006). *Redes privadas virtuales*. Recuperado de <http://www.uah.es/eh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20privadas%20virtuales.pdf>
- Hernández Sosa, B. H. & Valenzuela Cortez, O. A. (2013). *Desarrollo de un kit de herramientas digitales forense para la solución a problemas de Hardware y Software en el laboratorio de Hardware de la Universidad Tecnológica de El Salvador*. (Tesis de ingeniería). Universidad Tecnológica de El Salvador, San Salvador, SV. Recuperado de <http://biblioteca.utec.edu.sv/siab/virtual/tesis/66772.pdf>
- Infosegur. (2013). *Clasificación de seguridad*. Recuperado de <https://infosegur.wordpress.com/category/1-conceptos-basicos-de-la-seguridad-informatica/1-3-clasificacion-de-seguridad/>
- InfoSpyware. (2010). *10 consejos para navegar seguro por Internet*. Recuperado de <https://www.infospyware.com/articulos/10-consejos-para-navegar-seguro-por-internet/>
- Instituto nacional de estadística e informática (INEI). (2000). *Conceptos sobre seguridad de la información*. Recuperado de http://www.onpei.gob.pe/seguridad/seguridad2_archivos/Lib5120/Libro.pdf
- Kaspersky. (2016). *Amenazas móviles para Android*. Recuperado de <http://www.kaspersky.es/internet-security-center/threats/mobile>

- Kaspersky. (2016). *Riesgos de las redes WiFi públicas y por qué no debes temerlas*. Recuperado de <http://www.kaspersky.es/internet-security-center/internet-safety/public-wifi-risks#>
- KasperskyLab. (2016). *Seguridad para Smartphone*. Recuperado de <http://www.kaspersky.es/internet-security-center/internet-safety/smartphones>
- Luzardo, I. (2010). *Conozca las amenazas informáticas más comunes (DISI 2010)*. Recuperado de <http://www.enter.co/chips-bits/seguridad/conozca-las-amenazas-informaticas-mas-comunes-disi2010/>
- Mojsiejczuk, G. (2007). *Seguridad en los sistemas operativos*. Recuperado de <http://exa.unne.edu.ar/informatica/SO/Monogrgaby.pdf>
- Molina Rivera, Y. J.; Sandoval Cardona, J. & Toledo Franco, S. A. (2012). *Sistema operativo Android: características y funcionalidad*. Recuperado de <http://repositorio.utp.edu.co/dspace/bitstream/11059/2687/1/0053M722.pdf>
- NetWorkWorld. (2016). *Principales amenazas para la seguridad de las redes inalámbricas*. Recuperado de <http://www.networkworld.es/seguridad/principales-amenazas-para-la-seguridad-de-las-redes-inalambricas>
- Ochoa Ovalle, S. & Cervantes Sánchez, O. (2012). *Seguridad informática*. Recuperado de <http://www.eumed.net/rev/cccss/21/oocs.html>
- Panda Security. (2008). *Guía de herramientas de seguridad*. Recuperado de http://www.pandasecurity.com/NR/rdonlyres/DF1A6ACC-FABD-4E32-87AD-D35CA7B6B49C/0/Seguridad_hogares.pdf

- Pousa, A. (2011). *Algoritmo de cifrado simétrico AES. Aceleración de tiempo de cómputo sobre arquitecturas multicore*. Recuperado de http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Pousa_Adrian.pdf
- Radvan, S. (2010). *Guía de redes inalámbricas. (Wireless)*. Recuperado de https://docs.fedoraproject.org/es-ES/Fedora/13/pdf/Wireless_Guide/Fedora-13-Wireless_Guide-es-ES.pdf
- RedIRIS. (2002). *Seguridad física de los sistemas*. Recuperado de <https://www.rediris.es/cert/doc/unixsec/node7.html>
- Tarazona, C. (2007). *Amenazas informáticas y seguridad de la información*. Recuperado de <http://revistas.uexternado.edu.co/index.php/derpen/article/view/965/915>
- Welivesecurity. (2014). *Guía de seguridad para Smartphone: ¿Cómo configurar tu Android de la forma más segura?* Recuperado de http://www.welivesecurity.com/wp-content/uploads/2014/06/guia_seguridad_android_es

ANEXO

MATRIZ DE CONGRUENCIA		
TEMA: Desarrollo de un Kit de Seguridad Informática Enfocada para la Protección de la Información Computacional tanto en Hardware como en Software para la Universidad Tecnológica de El Salvador.		
ENUNCIADO DEL PROBLEMA: ¿De qué manera se podría proteger la información que manejan los estudiantes dentro los laboratorios de la Universidad Tecnológica de El Salvador?		
OBJETIVO GENERAL: Desarrollar un kit de seguridad informática para sistemas operativos Windows 7 o superior y Android 4.0 o superior enfocado a la protección de los datos informáticos que puedan ser utilizados por los estudiantes de la Universidad Tecnológica de El Salvador.		
OBJ.ESPECIFICO 1: Investigar los mejores softwares que se utilizaran para la seguridad informática analizarlos, instalarlos y comprobar si realmente protege, después de las pruebas crear fichas técnicas con características, requerimientos de instalación y especificaciones.	OBJ.ESPECIFICO 2: Crear un Kit con Herramientas que contengan los mejores softwares utilizados para la seguridad informática en un DVD multimedia.	OBJ.ESPECIFICO 3: Crear manual de software de seguridad informática el cual tendrá imágenes y procedimientos para instalar los softwares que estarán en el DVD multimedia.
PROMESA 1: Crear un manual de Seguridad Informática.	PROMESA 2: Investigar software que se utilizan en la seguridad informática	PROMESA 2: Desarrollar un kit de seguridad informática.
PRODUCTO 1: Manual impreso con información técnica de cómo se utilizar cada software, en su contenido tendrá capturas de pantalla con los pasos a seguir para instalar cada uno de los softwares.	PRODUCTO 2: Herramientas de software de seguridad informática con fichas técnicas.	PRODUCTO 3: Kit de seguridad informática multimedia.
DOCUMENTACIÓN TÉCNICA: Datos dblock Plus. Autor: Creado por Wladimir Palant en 2006. Licencia: Gratis		

Idioma: inglés y español)

REQUISITOS.

Sistema Operativo: Microsoft Windows 7 o superior, Linux y MAC OS.

Compatible con los siguientes navegadores: Mozilla Firefox, Google Chrome, Opera,

Datos BestCrypt Container Encryption.

Autor: Jetico Inc. Oy.

Licencia: \$ 59.95.

Idioma: español e inglés.

REQUISITOS.

Sistema operativo: Windows, Linux y MAC OS.

Datos HOTSPOT SHIELD.

Autor: AnchorFree Inc.

Licencia: Gratis y versión Hotspot Shield Elite de paga \$ 19.99 por 6 meses)

Idioma: español y varios idiomas.

REQUISITOS.

Sistema operativo: Windows, Androide, Linux y MAC OS

Datos FREE VPN PROXY.

Autor: Betternet Technologies Inc.

Licencia: gratis.

Idioma: español e inglés.

REQUISITOS.

Sistema Operativo: Android 4.0 o superior.

Nota: en algunos modelos no es compatible.

Datos ANDROID DEVICE MANAGER.

Autor: Google Inc.

Licencia: gratis.

Idioma: español e inglés.

REQUISITOS.

Sistema operativo: Android 4.0 o superior.

Nota: En algunos modelos no es compatible

Datos CERRADURA (APP LOCK).

Autor: DoMobile Ltd

Licencia: gratis.

Idioma: español.

REQUISITOS.

Sistema operativo: Android 4.0 o superior.

Nota: En algunos modelos no es compatible.

Datos AVG ANTIVIRUS FREE.

Autor: AVG Technologies CZ, s.r.o.

Licencia: gratis

Idioma: español.

Versiones:

REQUISITOS Sistema operativo: Windows 7 o superior, MAC OS y Android. Datos MALWAREBYTES. Autor: Malwarebytes Licencia: free y Premium \$ 24.95 por un año. Idioma: español. Sistema operativo: Windows 7 o superior, MAC OS y Android. Datos COMODO FIREWALL. Autor: Comodo Group, Inc. Licencia: gratis Idioma: español e inglés. REQUISITOS Sistema operativo: Windows vista, 7, 8,8.1 y 10.
PROYECTO TEMÁTICO: DESARROLLO DE UN KIT DE SEGURIDAD INFORMÁTICA ENFOCADA PARA LA PROTECCIÓN DE LA INFORMACIÓN COMPUTACIONAL TANTO EN HARDWARE COMO EN SOFTWARE PARA LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR.
DETALLES DEL PRESUPUESTO PROYECTADO: Programas de paga. BestCrypt Container Encryption \$ 59.95 Hotspot Shield Elite. \$ 19.99 (6 meses) AVG Antivirus 1 pc \$ 39.99 1 año MalwareBytes Premium 1 pc \$ 24.95 1 año
OFERTA ECONÓMICA: Programas de paga. BestCrypt Container Encryption \$ 59.95 Hotspot Shield Elite. \$ 19.99 (6 meses) AVG Antivirus 1 pc \$ 39.99 1 año MalwareBytes Premium 1 pc \$ 24.95 1 año

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

1

DECRETO N° 260

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR,
CONSIDERANDO:

I.- Que la Constitución de la República, reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común.

II.- Que mediante Decreto Legislativo N° 1030, de fecha 26 de abril de 1997, publicado en el Diario Oficial N° 105, Tomo N° 335, del 10 de junio del mismo año, se emitió el Código Penal.

III.- Que en la actualidad, los instrumentos electrónicos por medio de los cuales se envía, recibe o resguarda la información, han adquirido una especial relevancia, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural del país; por lo que se vuelve prioridad del Estado, proteger dicha información, ya que al no protegerla se atenta contra la confidencialidad, integridad, seguridad y disponibilidad de los datos en general.

IV.- Que esta diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación, no se encuentran suficientemente reguladas en nuestra normativa penal vigente, generándose una impunidad para quienes cometen estos tipos de delitos; en consecuencia, resulta

necesaria su tipificación y la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos.

POR TANTO,

en uso de sus facultades Constitucionales y a iniciativa del Diputado Douglas Leonardo Mejía Avilés,
de los Períodos Legislativos 2009 - 2012 y 2012 - 2015.

DECRETA, la siguiente:

LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS

TÍTULO I

DISPOSICIONES GENERALES

Objeto de la Ley

Art. 1.- La presente Ley tiene por objeto proteger los bienes jurídicos de aquellas conductas

delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la

prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o

transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

2

el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen

de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley.

Ámbito de Aplicación

Art. 2.- La presente Ley se aplicará a los hechos punibles cometidos total o parcialmente en el

territorio nacional o en los lugares sometidos a su jurisdicción. También se aplicará a cualquier persona,

natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus

habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador.

De igual forma, se aplicará la presente Ley si la ejecución del hecho, se inició en territorio

extranjero y se consumó en territorio nacional o si se hubieren realizado, utilizando Tecnologías de la

Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado

por el mismo hecho por Tribunales extranjeros o ha evadido el juzgamiento o la condena.

Definiciones

Art. 3.- Para los efectos de la presente Ley, se entenderá por:

a) Delito Informático: se considerará la comisión de este delito, cuando se haga uso de las

Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información;

b) Bien Jurídico Protegido: es la información que garantice y proteja el ejercicio de derechos

fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros;

c) Datos Informáticos: es cualquier representación de hechos, información o conceptos en

un formato digital o análogos, que puedan ser almacenados, procesados o transmitidos en un sistema informático, cualquiera que sea su ubicación, así como las características y especificaciones que permiten describir, identificar, descubrir, valorar y administrar los

datos;

d) Medio de Almacenamiento de Datos Informáticos: es cualquier dispositivo a partir del

cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo;

e) Sistema Informático: es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación

o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información;

f) Comunicación Electrónica: es toda transmisión de datos informáticos, cuyo contenido puede consistir en audio, texto, imágenes, videos, caracteres alfanuméricos, signos, gráficos de diversa índole o cualquier otra forma de expresión equivalente, entre un

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

3

remitente y un destinatario a través de un sistema informático y las demás relacionadas con las Tecnologías de la Información y la Comunicación;

g) Dispositivo: es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede

ser utilizado para ejecutar cualquier función de la Tecnología de la Información y la Comunicación;

h) Interceptar: es la acción de apropiarse, interrumpir, escuchar o grabar datos informáticos

contenidos o transmitidos en cualquier medio informático antes de llegar a su destino;

i) Programa Informático: es la rutina o secuencia de instrucciones en un lenguaje informático

determinado que se ejecuta en un sistema informático, pudiendo ser éste un ordenador, servidor o cualquier dispositivo, con el propósito que realice el procesamiento y comunicación de los datos informáticos;

j) Proveedor de Servicios: es la persona natural o jurídica que ofrece uno o mas servicios de información o comunicación por medio de sistemas informáticos, procesamiento o almacenamiento de datos;

k) Tráfico de Datos Informáticos: son aquellos que se transmiten por cualquier medio tecnológico, pudiendo mostrar el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación, entre otros;

l) Tecnologías de la Información y la Comunicación: es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros;

m) Datos Personales: es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar;

n) Datos Personales Sensibles: son los que corresponden a una persona en lo referente al

credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias

sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la propia imagen, a la intimidad personal y familiar;

o) Material Pornográfico de Niñas, Niños y Adolescentes: es toda representación auditiva

o visual, ya sea en imagen o en vídeo, adoptando un comportamiento sexualmente explícito, real o simulado de una persona que aparente ser niña, niño o adolescente adoptando tal comportamiento. También se considerará material pornográfico, las imágenes realistas que representen a una niña, niño o adolescente adoptando un comportamiento sexualmente explícito o las imágenes reales o simuladas de las partes

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

4

genitales o desnudos de una niña, niño o adolescente con fines sexuales;

p) Tarjeta Inteligente: es el dispositivo que permite mediante la ejecución de un programa

la obtención de bienes, servicios, propiedades o información; y,

q) Redes Sociales: es la estructura o comunidad virtual que hace uso de medios tecnológicos

y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación, mediante el intercambio de información.

TÍTULO II

DE LOS DELITOS

CAPÍTULO I

DE LOS DELITOS CONTRA LOS SISTEMAS TECNOLÓGICOS DE INFORMACIÓN

Acceso Indebido a Sistemas Informáticos

Art. 4.- El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido,

acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la

Información o la Comunicación, será sancionado con prisión de uno a cuatro años.

Acceso Indebido a los Programas o Datos Informáticos

Art. 5.- El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de

la Información o la Comunicación, accediera parcial o totalmente a cualquier programa o a los datos

almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será

sancionado con prisión de dos a cuatro años.

Interferencia del Sistema Informático

Art. 6.- El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de

un sistema informático, de forma temporal o permanente, será sancionado con prisión de tres a cinco

años.

Se considerará agravada la interferencia o alteración, si ésta recayera en programas o sistemas

informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de

comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público,

o destinados a la prestación de servicios financieros, la sanción de prisión será de tres a seis años.

Daños a Sistemas Informáticos

Art. 7.- El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere

el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice las Tecnologías de

la Información y la Comunicación o cualquiera de los componentes que las conforman, será sancionado con prisión de tres a cinco años.

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

5

Si el delito previsto en el presente artículo se cometiere de forma culposa, por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, será sancionado con prisión de uno a tres años.

Si el delito previsto en el presente artículo se cometiere en contra de cualquiera de los componentes de un sistema informático que utilicen las Tecnologías de la Información y la Comunicación, que estén destinadas a la prestación de servicios públicos o financieros, o que contengan información personal, confidencial, reservada, patrimonial, técnica o propia de personas naturales o jurídicas, la sanción de prisión será de tres a seis años.

Posesión de Equipos o Prestación de Servicios para la Vulneración de la Seguridad

Art. 8.- El que utilizando las Tecnologías de la Información y la Comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado con prisión de tres a cinco años.

Violación de la Seguridad del Sistema

Art. 9.- La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionado con prisión de tres a seis años.

En igual sanción incurrirá quien induzca a un tercero para que de forma involuntaria, ejecute un

programa, mensaje, instrucciones o secuencias para violar medidas de seguridad.

No incurrirá en sanción alguna quien ejecute las conductas descritas en los Arts. 8 y 9 inciso

primero de la presente Ley, cuando con autorización de la persona facultada se realicen acciones con el

objeto de conducir pruebas técnicas o auditorías de funcionamiento de equipos, procesos o programas.

CAPÍTULO II

DE LOS DELITOS INFORMÁTICOS

Estafa informática

Art. 10.- El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de

un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de

datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación

informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos

del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u

obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco

años.

Se sancionará con prisión de cinco a ocho años, si las conductas descritas en el inciso anterior

se cometieren bajo los siguientes presupuestos:

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

6

- a) En perjuicio de propiedades del Estado;
- b) Contra sistemas bancarios y entidades financieras; y,
- c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos.

Fraude Informático

Art. 11.- El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años.

Espionaje Informático

Art. 12.- El que con fines indebidos obtenga datos, información reservada o confidencial

contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años.

Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión.

Hurto por Medios Informáticos

Art. 13.- El que por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de dos a cinco años.

Técnicas de Denegación de Servicio

Art. 14.- El que de manera intencionada, utilizando las técnicas de la denegación de servicio o prácticas equivalentes que afectaren a los usuarios que tienen pertenencia en el sistema o red afectada, imposibilite obtener el servicio, será sancionado con prisión de tres a cinco años.

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

7

CAPÍTULO III

DELITOS INFORMÁTICOS RELACIONADOS

CON EL CONTENIDO DE LOS DATOS

Manipulación de Registros

Art. 15.- Los Administradores de las Plataformas Tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro de acceso, uso de los componentes de éstos, será sancionado con prisión de cinco a ocho años.

Si las conductas descritas en el inciso anterior, favorecieren la comisión de otro delito, la sanción

se agravará hasta en una tercera parte del máximo señalado.

Manipulación Fraudulenta de Tarjetas Inteligentes o Instrumentos Similares

Art. 16.- El que intencionalmente y sin la debida autorización por cualquier medio cree, capture,

grave, copie, altere, duplique, clone o elimine datos informáticos contenidos en una tarjeta inteligente

o en cualquier instrumento destinado a los mismos fines; con el objeto de incorporar, modificar usuarios,

cuentas, registros, consumos no reconocidos, la configuración actual de éstos o de los datos en el sistema,

será sancionado con prisión de cinco a ocho años.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores adquiera,

comercialice, posea, distribuya, venda, realice cualquier tipo de intermediación de tarjetas inteligentes

o instrumentos destinados al mismo fin o de datos informáticos contenidos en ellos o en un sistema.

Obtención Indebida de Bienes o Servicios por Medio de Tarjetas Inteligentes o Medios

Similares

Art. 17.- El que sin autorización utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, utilice indebidamente las Tecnologías de la Información y la Comunicación para la obtención de cualquier bien o servicio, realice cualquier tipo de pago sin erogar o asumir obligación alguna por la contraprestación obtenida, será sancionado con prisión de tres a ocho años.

Provisión Indebida de Bienes o Servicios

Art. 18.- El que sin justificación, a través de un sistema informático utilice tarjetas inteligentes o instrumentos similares destinados a los mismos fines, cuya vigencia haya caducado o haya sido revocada por la institución que la emitió, o que se haya obtenido con el fin de suplantar la identidad contenida en dichas tarjetas inteligentes, será sancionado con prisión de cinco a ocho años.

El que falsifique o altere los datos de las tarjetas inteligentes o instrumentos similares, con el fin de proveer a quien los presente, dinero, bienes o servicios, o cualquier otro objeto de valor económico, la sanción aumentará hasta una tercera parte del máximo de la pena prevista en el inciso anterior.

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

8

Alteración, Daño a la Integridad y Disponibilidad de los Datos

Art. 19.- El que violando la seguridad de un sistema informático destruya, altere, duplique,

inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y

confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento,

será sancionado con prisión de tres a seis años.

Interferencia de Datos

Art. 20.- El que interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos

e ineficaces, para alterar o destruir los datos de un tercero, será sancionado con prisión de tres a seis

años.

Si alguna de las conductas descritas en el inciso anterior recae sobre datos, documentos, programas o sistemas informáticos públicos o sobre datos destinados a la prestación de servicios de salud,

de comunicaciones, sistemas bancarios, entidades financieras, de provisión y transporte de energía, de medios de transporte u otro servicio público, la sanción de prisión será de cinco a ocho años.

Interceptación de Trasmisiones entre Sistemas de las Tecnologías de la Información y la Comunicación

Art. 21.- La persona que sin justificación intercepte por medios tecnológicos cualquier transmisión hacia, desde o dentro de un sistema informático que no está disponible al público; o las emisiones electromagnéticas que están llevando datos de un sistema informático, será sancionada con prisión de siete a diez años.

Hurto de Identidad

Art. 22.- El que suplantare o se apoderare de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años.

Si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza

a otra persona para ocasionar perjuicio u obtener beneficios para si mismo o para terceros y el

apoderamiento recae sobre datos personales, confidenciales o sensibles definidos en la Ley de Acceso

a la Información Pública, será sancionado con prisión de cinco a ocho años.

Divulgación No Autorizada

Art. 23.- El que sin autorización da a conocer un código, contraseña de acceso o cualquier otro

medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin

de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho

años.

Igual sanción tendrá el que sin autorización revele o difunda los datos o información, contenidos

en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro.

Si alguna de las conductas descritas en los incisos anteriores pusieren en peligro la seguridad del

Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las

personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter

reservado, será sancionado con prisión de seis a doce años.

Utilización de Datos Personales

Art. 24.- El que sin autorización utilice datos personales a través del uso de las Tecnologías de

la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando

o modificando los datos en perjuicio de un tercero, será sancionado con prisión de cuatro a seis años.

La sanción aumentará hasta en una tercera parte del máximo de la pena prevista en el inciso

anterior a quien proporcione o revele a otro, información registrada en un archivo o en un banco de datos

personales cuyo secreto estuviere obligado a preservar.

Obtención y Transferencia de Información de Carácter Confidencial

Art. 25.- El que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años.

Revelación Indevida de Datos o Información de Carácter Personal

Art. 26.- El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años. Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años. Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte,

si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos

personales confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública.

Acoso a través de Tecnologías de la Información y la Comunicación

Art. 27.- El que realice conducta sexual indeseada por quien la recibe, que implique frases, señas

u otra conducta inequívoca de naturaleza o contenido sexual, por medio del uso de las Tecnologías de

la Información y la Comunicación, será sancionado con prisión de cuatro a seis años.

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

10

CAPÍTULO IV

DELITOS INFORMÁTICOS CONTRA NIÑAS, NIÑOS Y

ADOLESCENTES O PERSONAS CON DISCAPACIDAD

Pornografía a través del Uso de Tecnologías de Información y la Comunicación

Art. 28.- El que por cualquier medio que involucre el uso de las Tecnologías de la Información

y la Comunicación fabrique, transfiriera, difunda, distribuya, alquile, venda, ofrezca, produzca, ejecute,

exhiba o muestre material pornográfico, sexual entre niñas, niños y adolescentes o personas con

discapacidad, será sancionado con prisión de cuatro a ocho años.

Quien no advierta de forma visible el contenido del material pornográfico o sexual que se

transmita mediante el uso de las Tecnologías de la Información y la Comunicación, no apto para niñas,

niños, adolescentes o personas con discapacidad, será sancionado con prisión de tres a cinco años.

Utilización de Niñas, Niños, Adolescentes o Personas con Discapacidad en Pornografía a través

del Uso de las Tecnologías de la Información y la Comunicación

Art. 29.- El que por cualquier medio que involucre el uso de las Tecnologías de la Información

y la Comunicación produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda,

comercie o difunda de cualquier forma, imágenes, videos o exhiba en actividades sexuales, eróticas o

inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, o utilice la voz de niñas, niños,

adolescentes o personas con discapacidad, será sancionado con prisión de ocho a doce años.

Igual sanción se impondrá a quien por medio de las Tecnologías de la Información y la Comunicación organice o participe en espectáculos públicos o privados, en los que se hace participar a las personas señaladas en el inciso anterior, en acciones pornográficas o eróticas.

Adquisición o Posesión de Material Pornográfico de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación

Art. 30.- El que adquiriera para sí o para un tercero a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, o posea material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción, será sancionado con prisión de dos a cinco años.

Igual sanción se aplicará al que posea en dispositivos de almacenamiento de datos informáticos o a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación,

material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción.

Corrupción de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación

Art. 31.- El que mantenga, promueva o facilite la corrupción de una niña, niño, adolescente o persona con discapacidad con fines eróticos, pornográficos u obscenos, por medio de las Tecnologías de

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

11

la Información y la Comunicación, aunque la niña, niño, adolescente o persona con discapacidad lo consienta, será sancionado con prisión de ocho a doce años. Igual sanción se impondrá a quien haga propuestas implícitas o explícitas para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía a través del uso de las Tecnologías de

la Información y la Comunicación para sí, para otro o para grupos, con una niña, niño, adolescente o persona con discapacidad.

Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las

Tecnologías de la Información y la Comunicación

Art. 32.- Quien atormente, hostigue, humille, insulte, denigre u otro tipo de conducta que afecte

el normal desarrollo de la personalidad, amenace la estabilidad psicológica o emocional, ponga en riesgo

la vida o la seguridad física, de un niño, niña, adolescente o persona con discapacidad, por medio del uso

de las Tecnologías de la Información o Comunicación, será sancionado con prisión de dos a cuatro años.

La pena se agravará con prisión de cuatro a ocho años, para quien realice conducta que implique

frases, señas u otra acción inequívoca de naturaleza o contenido sexual contra una niña, niño, adolescente

o persona con discapacidad, por medio del uso de las Tecnologías de la Información y la Comunicación.

Condiciones Agravantes Comunes

Art. 33.- Los delitos referidos en el presente Capítulo, serán sancionados con la pena máxima

correspondiente, aumentada hasta en una tercera parte del máximo establecido de la pena y la

inhabilitación del ejercicio de su profesión durante el tiempo que dure la condena, si cualquiera de las

acciones descritas fuera realizada por:

a) Ascendientes, descendientes, hermanos, adoptantes, adoptados, cónyuges, conviviente

y familiares hasta el cuarto grado de consanguinidad y segundo de afinidad;

b) Funcionarios, empleados públicos y municipales, autoridad pública y agente de autoridad;

c) La persona encargada de la tutela, protección o vigilancia de la víctima; y,

d) Toda persona que prevaliéndose de la superioridad originada por relaciones de confianza,

doméstica, educativa, de trabajo o cualquier otra relación.

CAPÍTULO V

DELITO CONTRA EL ORDEN ECONÓMICO

Suplantación en Actos de Comercialización

Art. 34.- El que sin autorización y a nombre de un tercero, mediante el uso de las Tecnologías

de la Información y la Comunicación, venda o comercialice bienes o servicios, suplantando la identidad

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

12

del productor, proveedor o distribuidor autorizado, será sancionado con prisión de tres a cinco años.

La conducta descrita en el inciso anterior se agravará con pena de prisión de cuatro a seis años,

cuando la venta o comercialización se trate de medicamentos, suplementos o productos alimenticios,

bebidas o cualquier producto de consumo humano.

TÍTULO III

DISPOSICIONES FINALES

Otras Responsabilidades

Art. 35.- Las sanciones previstas en la presente Ley, serán aplicables sin perjuicio de otras

responsabilidades penales, civiles o administrativas en que se incurra.

Para la deducción de la responsabilidad civil se estará a lo dispuesto en la normativa aplicable.

Vigencia

Art. 36.- El presente Decreto entrará en vigencia ocho días después de su publicación en el Diario Oficial.

DADO EN EL SALÓN AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los cuatro días del mes de febrero del año dos mil dieciséis.

LORENA GUADALUPE PEÑA MENDOZA,
PRESIDENTA.

GUILLERMO ANTONIO GALLEGOS NAVARRETE, ANA VILMA ALBANEZ DE
ESCOBAR,

PRIMER VICEPRESIDENTE. SEGUNDA VICEPRESIDENTA.

JOSÉ SERAFÍN ORANTES RODRÍGUEZ, NORMAN NOEL QUIJANO
GONZÁLEZ,

TERCER VICEPRESIDENTE. CUARTO VICEPRESIDENTE.

SANTIAGO FLORES ALFARO,

QUINTO VICEPRESIDENTE.

GUILLERMO FRANCISCO MATA BENNETT, DAVID ERNESTO REYES
MOLINA,

PRIMER SECRETARIO. SEGUNDO SECRETARIO.

MARIO ALBERTO TENORIO GUERRERO, REYNALDO ANTONIO LÓPEZ
CARDOZA,

TERCER SECRETARIO. CUARTO SECRETARIO.

JACKELINE NOEMÍ RIVERA ÁVALOS, JORGE ALBERTO ESCOBAR BERNAL,

QUINTA SECRETARIA. SEXTO SECRETARIO.

INDICE LEGISLATIVO

ASAMBLEA LEGISLATIVA - REPUBLICA DE EL SALVADOR

13

ABILIO ORESTES RODRÍGUEZ MENJÍVAR, JOSÉ FRANCISCO MERINO
LÓPEZ,

SÉPTIMO SECRETARIO. OCTAVO SECRETARIO.

CASA PRESIDENCIAL: San Salvador, a los veintiséis días del mes de febrero del año
dos mil

dieciséis.

PUBLÍQUESE,

Salvador Sánchez Cerén,

Presidente de la República.

Mauricio Ernesto Ramírez Landaverde,

Ministro de Justicia y Seguridad Pública.

D. O. N° 40

Tomo N° 410

Fecha: 26 de febrero de 2016

SV/ielp

30-03-2016

INDICE LEGISLATIVO (Asamblea Legislativa de El Salvador, 2016)