

Ciberseguridad en el ejercicio del periodismo

David Perera

Licencia: CC BY-NC-SA

Atribución-NoComercial-CompartirIgual

Septiembre 2016

<http://mx.usembassy.gov/es/mty/ciberseguridad>

Agradecimientos

Esta presentación forma parte de una serie de seminarios “Free the Press” patrocinada por el Consulado de Estados Unidos en Monterrey.

Puedes descargar presentaciones y ver grabaciones de todas las sesiones desde este sitio web:

<https://mx.usembassy.gov/es/embajada-y-consulados-de-eu/monterrey/free-press-seminar-series/>

Descarga esta presentación directamente desde aquí:

<http://mx.usembassy.gov/es/mtty/ciberseguridad>

Introducción

¿Por qué la seguridad y el anonimato?

- Como periodistas, hay gente que quiere saber con quién hablamos, quienes son nuestros fuentes de información. ¿Qué hacemos? ¿Qué sabemos?
- Tenemos el ejemplo reciente de Rafael Cabrera, el reportero quien reveló la controversia sobre la “Casa Blanca” de Presidente Enrique Peña Nieto.

Ciberespionaje a periodistas

POR JORGE CARRASCO Y MATHIEU TOURLIERE , 30 AGOSTO, 2016

REPORTAJE ESPECIAL



CIUDAD DE MÉXICO (Proceso).- Heredera de la tecnología invasiva que adquirió el gobierno de Felipe Calderón, la administración de Peña Nieto ha mantenido el ciberespionaje como una de sus herramientas políticas. Entre sus objetivos, hasta ahora mencionados, han sido periodistas y activistas.

El caso más reciente es el del reportero Rafael Cabrera, de Aristegui Noticias, quien inició la investigación de la Casa Blanca y recientemente firmó el trabajo sobre el plagio de la tesis de licenciatura de Peña Nieto.

<http://www.proceso.com.mx/452866/ciberespionaje-a-periodistas>

¡Advertencia!

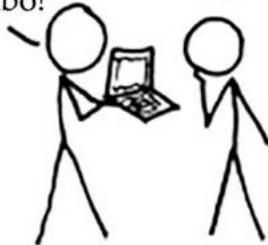
- Todo de lo que hablaremos hoy es solo el primer paso.
- Aunque si tomes todas las precauciones necesarias de seguridad y anonimato en el ciberespacio, aún sigues siendo un ser físico.
- Ningún programa ni ningún hardware es totalmente seguro.

Desde la imaginación
de un cibernerdo:

Su portátil está encriptado. Construye
una supercomputadora para romper
el código.

¡Inútil! ¡Utilizó
4096-BIT RSA!

¡Maldición! ¡Nuestro plan
maligno se acabó!



Lo que en realidad
pasaría:

Su portátil está encriptado.
Golpealo con esta llave inglesa
hasta que hable.

Entendido.



<https://xkcd.com/538/>

Desafíos

- Tu editor no apoya tus esfuerzos para estar más seguro.
- No tienes control suficiente sobre tu equipo. Necesitas la habilidad de poder descargar desde el internet aplicaciones nuevas y permisos para ajustar las configuraciones de tu computadora y tu móvil.
- La presión de cerrar la edición confronta con la seguridad, que exige más tiempo que la inseguridad.
- Tentación general de omitir pasos que son necesarios para la seguridad o anonimato, porque mantener los dos diariamente puede ser una pena. El nivel de protección que pones en marcha depende de la fuerza del riesgo.
- Insuficiente ancho de banda de acceso.

Antes de todo

- Establecer un *modelo de riesgos*. No todo el mundo tiene las mismas prioridades o ven las amenazas de la misma manera.
- ¿Qué es lo que estás protegiendo?
- ¿Quién quiere tus datos o quiere interceptar tus comunicaciones?
- ¿Cuán probable es que necesites protegerlos?
- ¿Cuáles métodos tienen los adversarios para obtener tus bienes digitales?
- ¿Cuán destructivas pueden ser las consecuencias si fallas?

- ¿Puedo confiar en proveedores de servicios en línea?
- Las compañías más grandes de tecnología como Google, Apple, Microsoft, Twitter y Facebook publican informes de transparencia (todos debajo en español, menos Microsoft y DropBox)
 - Google: <https://www.google.com/transparencyreport/?hl=es>
 - Apple: <http://www.apple.com/es/privacy/transparency-reports/>
 - Microsoft: <https://www.microsoft.com/about/csr/transparencyhub/lerr/>
 - Twitter: <https://transparency.twitter.com/es/home>
 - Facebook: https://es-la.facebook.com/about/government_requests
 - DropBox: <https://www.dropbox.com/transparency>
- Por ejemplo, en la segunda mitad de 2015, Google dice que cumplió con 54% de solicitudes mexicanas legales para revelar información sobre usuarios.
<https://www.google.com/transparencyreport/userdatarequests/MX/>

Conceptos básicos: El anonimato y la ciberseguridad

- Los dos, aunque están vinculados, no son iguales.
- El anonimato es actuar o comunicarse sin usar o presentar el nombre o identidad propia.
- La ciberseguridad es tomar medidas para proteger tu información y evitar que otros pueden controlar sin tu conocimiento tus dispositivos para fines de espionaje o daño.

Conceptos básicos: datos y metadatos

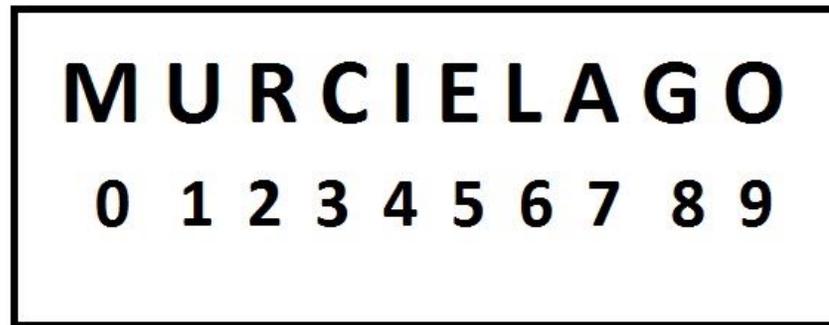
- Metadatos literalmente significa “datos sobre datos”. El contenido de comunicaciones es considerado “datos” mientras información como **el asunto, la cuenta de correo** electrónico que envió el mensaje y la cuenta que lo recibió, **la dirección en línea** de la computadora que envió el mensaje (y que lo recibió), la fecha y hora del mensaje – todos son metadatos
- Los metadatos también existen en archivos, como **el autor** de documento y **la fecha** de creación.
- Si se trata de una foto, los metadatos son **la fecha, la hora y el minuto** en que la foto fue tomada, **la marca y el modelo de la cámara** y hasta **las coordenadas GPS** de la ubicación en que la foto fue tomada (especialmente, si la foto fue tomada por un móvil).
- Con móviles o teléfonos, los metadatos son **los números que llamas** o a que envías un mensaje como un texto de SMS, **los números que te llaman** o dan mensajes, **y tu locación**.
- Generalmente, es mucho más fácil por un gobierno obtener los metadatos que los datos. Pero con metadatos, se sabe con **quién te comunicas, con cual frecuencia** hasta **en cual lugar estuviste**.

Conceptos básicos: dirección IP

- IP es “protocolo de internet”, IP por las siglas en inglés (“Internet protocol”)
- Es la dirección virtual de tu dispositivo en el internet y es otro ejemplo de metadatos.
- Aquí un ejemplo: 23.196.106.96. Puedes Googlear “¿Cuál es mi dirección IP?” para ver la tuya.
- La dirección IP no es estática—no forma parte permanente de tu computadora o móvil. La dirección cambia cada vez que conectas a una nueva red. La dirección está asignada al dispositivo por el proveedor de servicios de internet.
- Cuando se conecta a un sitio web u otro servicio en línea, revelas tu dirección IP a todas las computadoras entre tú y del sitio web o servicio en línea, y por supuesto al destino final.

Conceptos básicos: encriptación

- Encriptación convierte con una clave especial mensajes (incluso llamadas) o archivos claramente legibles a una forma cuyo significado es inentendible a los demás que no conocen la clave.



Plátanos = P67t7n9s Bolígrafo = B964827f9

- Lo fundamental de utilizar cualquier aplicación que pretende encriptar mensajes es saber quién controla las claves.
- Cuando las claves están bajo el control solamente del usuario y no del proveedor, eso es encriptación punto-a-punto (también llamado encriptación de extremo-a-extremo) y es la moda más segura.
- Si el proveedor mantiene control de las claves por su parte, corres el riesgo que el proveedor dé el contenido de tus mensajes o archivos al gobierno u otro tercero.

El sentido común nos dice
que la tierra debe ser plana

Medidas fundamentales para la ciberseguridad

Contra ataques de phishing:

- Phishing sigue siendo el método más común para infectar equipo.
- Phishing se produce cuando un atacante envía un enlace (a través de correo electrónico, chat o SMS) que parece inofensivo pero que realmente es malicioso. Un ataque exitoso – cuando cliques el enlace – típicamente abre en software espía y lo instala en tu computadora o móvil sin tu conocimiento.
- Otra variación es cuando el enlace te manda a un pantalla de inicio por un servicio como Google que parece legítimo pero en verdad es una réplica malicioso que graba tus datos de acceso y contraseñas.
- Sin duda has oído esto anteriormente, pero vale la pena repetirlo: No cliques enlaces sospechosos.
- ¿Cómo reconocer enlaces sospechosos? Veamos al ejemplo de Rafael Cabrera.

< Mensajes (81) 2095 3203 Detalles

Mensaje de texto
hoy 10:46 a.m.

[TELCEL.COM/](#)
ESTIMADO USUARIO
LE RECORDAMOS QUE
PRESENTA UN
ADEUDO DE \$8,854.90
M/N VERIFIQUE
DETALLES: [https://
ideas-telcel.com.mx/
3975827s/](https://ideas-telcel.com.mx/3975827s/)

- Este enlace no pertenece a Telcel.com, aunque “Telcel.com” forma parte del enlace.
- Los atacantes esperan que sólo ves rápidamente que “Telcel.com” forma parte del enlace para que lo cliques.

< Mensajes (81) 2075 4118 Detalles

Mensaje de texto
hoy 11:50 a.m.

Facebook reporta intentos de acceso a la cuenta: Rafa Cabrera. Evite bloqueo de cuenta, verifique en: <https://fb-accounts.com/2408931s/>

Si recibes un mensaje semejante – algo como “Su cuenta bancaria está sobregirada, inicie sesión aquí”, no cliques nunca el enlace. En vez, ve directamente al sitio en línea de tu banco, de Facebook, etc., para comprobar si existe dicho problema.



(313) 105 1501 *ahora*

No tienes los huevos de ver como me fajo a tu pareja. Mira nada mas como cojemos bn rico y en tu cama: <http://bit.ly/246dkRy>

El propósito aquí es que te enojas para que cliques el enlace sin pensarlo. Y han ocultado la dirección verdadera (y maligna) con un acortador de enlaces.

- Si alguien te manda un enlace acortado y no estás seguro a quien pertenece, puedes chequearlo aquí: <http://unfurlr.com/> o aquí: <http://www.checkshorturl.com/>
- Estos sitios deshacen el acortamiento y muestran cual es el enlace verdadero.

The screenshot shows the unfurlr.com interface. At the top, there is a blue header with the unfurlr logo and a "Disclaimer" button. Below the header, the text "What's behind that short link?" is displayed. A search bar labeled "Check this URL" contains the text "http://bit.ly/2cfqFV2". Below the search bar is a blue "Check It" button and a link for "Advanced Options". A large red arrow points from the "Check It" button to the "Results" section. The "Results" section is titled "Results" and contains a yellow box labeled "We Ended Up Here" with the URL "http://aristeguinoticias.com/0209/kiosko/alistan-ruta-de-la-cerveza-artesanal-de-la-cdmx-a-tlaxcala/".

- Una etapa más si tienes dudas sobre la validez del enlace: comprueba lo con Google, que examina enlaces para la seguridad.

- Haz lo aquí:

<https://www.google.com/transparencyreport/safebrowsing/diagnostic/index.html?hl=es>

Google Informe de transparencia

Página principal Tráfico Solicitudes de retirada de contenido Seguridad y privacidad

Solicitudes de información sobre nuestros usuarios Navegación segura Correo electrónico más seguro HTTPS

Descripción general

Panel de software malicioso

Estado del sitio web

Notas

Preguntas frecuentes

Estado del sitio según Navegación segura

La tecnología Navegación segura de Google examina miles de millones de URL todos los días en busca de sitios web no seguros. A diario descubrimos miles de sitios no seguros nuevos, muchos de los cuales son sitios web legítimos que se han puesto en peligro. Cuando detectamos sitios no seguros, mostramos advertencias en la Búsqueda de Google y en los navegadores web. Puedes realizar búsquedas para ver si es peligroso visitar un sitio web.

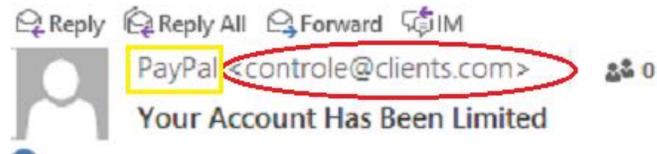
Estado de:

Estado actual: No peligroso

Navegación segura no ha detectado recientemente contenido malicioso en el sitio aristeguinoticias.com.

- Pero ojo, es aún posible que el enlace sea peligroso y Google no ha logrado todavía darse cuenta.

- Quizás recibes un enlace un tanto sospechoso pero parece que un amigo, un socio o tu jefe te lo mandó. Correos electrónicos pueden ser engañosos, porque el nombre el escritor puede aparecer como alguien a quien conoces a pesar del hecho que el mensaje fue verdaderamente mandado por un extraño. Verifica no solo el nombre del remitente, sino la dirección verdadera.



- También, no abras adjuntos extraños. Es método común para implantar aplicaciones de vigilancia.

Medidas expertas para la ciberseguridad

Medidas por ciberseguridad más comunes con inexpertos	vs	Medidas por ciberseguridad más comunes con expertos
El uso de antivirus 		Instalar actualizaciones de software 
Contraseñas fuertes 		Contraseñas únicas 
Cambiar contraseñas con frecuencia 		Autenticación de dos factores 
Sólo ir a sitios web previamente conocidos 		Contraseñas fuertes 
No compartir datos personales 		Utilizar un gestor de contraseñas 

<https://security.googleblog.com/2015/07/new-research-comparing-how-security.html>

Medidas expertas: Actualizaciones de software

- Las cosas que los inexpertos hacen no son todas incorrectas – antivirus sigue siendo una herramienta fundamental (por computadoras sí, pero por móviles no son necesarios).
- ¿Por qué dicen los expertos que lo más importante es instalar actualizaciones de software? Porque saben que el antivirus es inútil cuando se trata de ataques no previstos, un tipo de ataque que aprovecha las vulnerabilidades nuevas, que se llama un ataque de “día cero”.
- Un día cero está llamado así porque los vendedores de software y de antivirus han tenido ceros días para crear una defensa. Estas defensas llegan al usuario en forma de actualizaciones periódicas – y es por eso que los expertos no pierden tiempo en instalar cada actualización nueva.

Medidas expertas: Contraseñas

- Tener una contraseña fuerte es importante. Los expertos como lo inexpertos creen en su importancia.
- Pero más importante para expertos es que cada cuenta tenga una contraseña única. Si tienes la misma contraseña para tu correo electrónico, tu banco, tus redes sociales, etc., has creado una la clave para abrir todos cuentas tuyas.
- ¿Qué es una contraseña fuerte? Son largas – 14 caracteres mínimo y caracteres escogidas al azar, con letras mayúsculas y minúsculas, números y caracteres especiales.
- Una contraseña no puede ser basada en una palabra.
- Por ejemplo: “XgYH85@L23P9b#” y no “c0ntr@señ@1234”.

- ¿Cómo recordar contraseñas fuertes?
- La solución es utilizar un gestor de contraseñas (también llamado una billetera digital para contraseñas), que es una aplicación para manejar contraseñas. Con esa aplicación, el software genera y recuerda contraseñas fuertes para ti. Así hay que recordar solo una contraseña, la contraseña maestra que abre la aplicación.
- LastPass (<https://lastpass.com/es/>) y dashlane (<https://www.dashlane.com/es/>) son buenos gestores. Los dos ofrecen versiones gratuitas.
- Hay un gestor de código abierto y totalmente gratuito llamado KeePassX (<http://keepass.info/>) Para ayuda con KeePassX, visita este enlace: <https://ssd.eff.org/es/module/c%C3%B3mo-usar-keepassx>

- ¿Cómo escoger la contraseña maestra del gestor u otras contraseñas para que no sirve un gestor de contraseñas (una contraseña para el inicio de sesión de un portátil, por ejemplo)?
- Hay un método llamado “edadosí”.
- Se necesita dos cosas: una lista de palabras que corresponde a un código de cinco números, y cinco dados.
- En la lista de palabras, cada palabra corresponde a un número hecho de cinco dígitos. Entonces, cada vez que tiras cinco dados, tienes una palabra nueva.
- Por ejemplo, tiro
52634 | 15662 | 43223 | 22512 | 22212
- En la lista, estos números significan:
Otro | ¿?? | Lama | s96 | algo

- Y así llego a esta contraseña:
otro¿??Lamas96algo
- Si pones espacios o más caracteres entre las palabras, la contraseña es aún más fuerte
Otro ¿?? Lama s96 algo
Otro*¿??*Lama*s96*algo
- Puedes leer más sobre edadosí aquí:
http://world.std.com/%7Ereinhold/diceware_en_espanolA.htm
- Y encuentras listas de palabras en español aquí:
http://world.std.com/~reinhold/diceware_espanol/DW-Espanol-1.txt
http://world.std.com/~reinhold/diceware_espanol/DW-Espanol-2.txt

Medidas expertas: Autenticación de dos factores

- Cuando usas un gestor de contraseñas, la seguridad de tus contraseñas y la contraseña maestra sólo es tan sólida como la seguridad de tu equipo. Si tus dispositivos están infectados con malware de espionaje, el atacante puede verte escribir la contraseña maestra y robarte el contenido de gestor.
- Puedes tomar medidas para fortalecer la seguridad de la contraseña maestra y la seguridad de todos de tus cuentas mediante el uso de autenticación de dos factores.
- **Autenticación de dos factores:** cuando el usuario se identifica a un proveedor de servicios por medio de una combinación de dos diferentes métodos.
- Por ejemplo, una contraseña y un código único generado por una aplicación móvil o una contraseña y la presencia de un llave de seguridad como un dispositivo físico USB.

Aplicación móviles

- Google Authenticator:: <https://support.google.com/accounts/answer/1066447?hl=es>
- Authy
iPhone: <https://itunes.apple.com/us/app/authy/id494168017?mt=8>
Android: <https://play.google.com/store/apps/details?id=com.authy.authy&hl=es>

Dispositivos físicos USB

- Una empresa californiana fabrica los mejores: Yubico
 - Envía productos a todos países y venden una versión que cuesta US \$18 (aproximado MXN \$360)
 - <https://www.yubico.com/products/yubikey-hardware/fido-u2f-security-key/>

Consulta Apéndice A para ver como establecer autenticación de dos factores con Authy o Google Authenticator con tu cuenta de Google



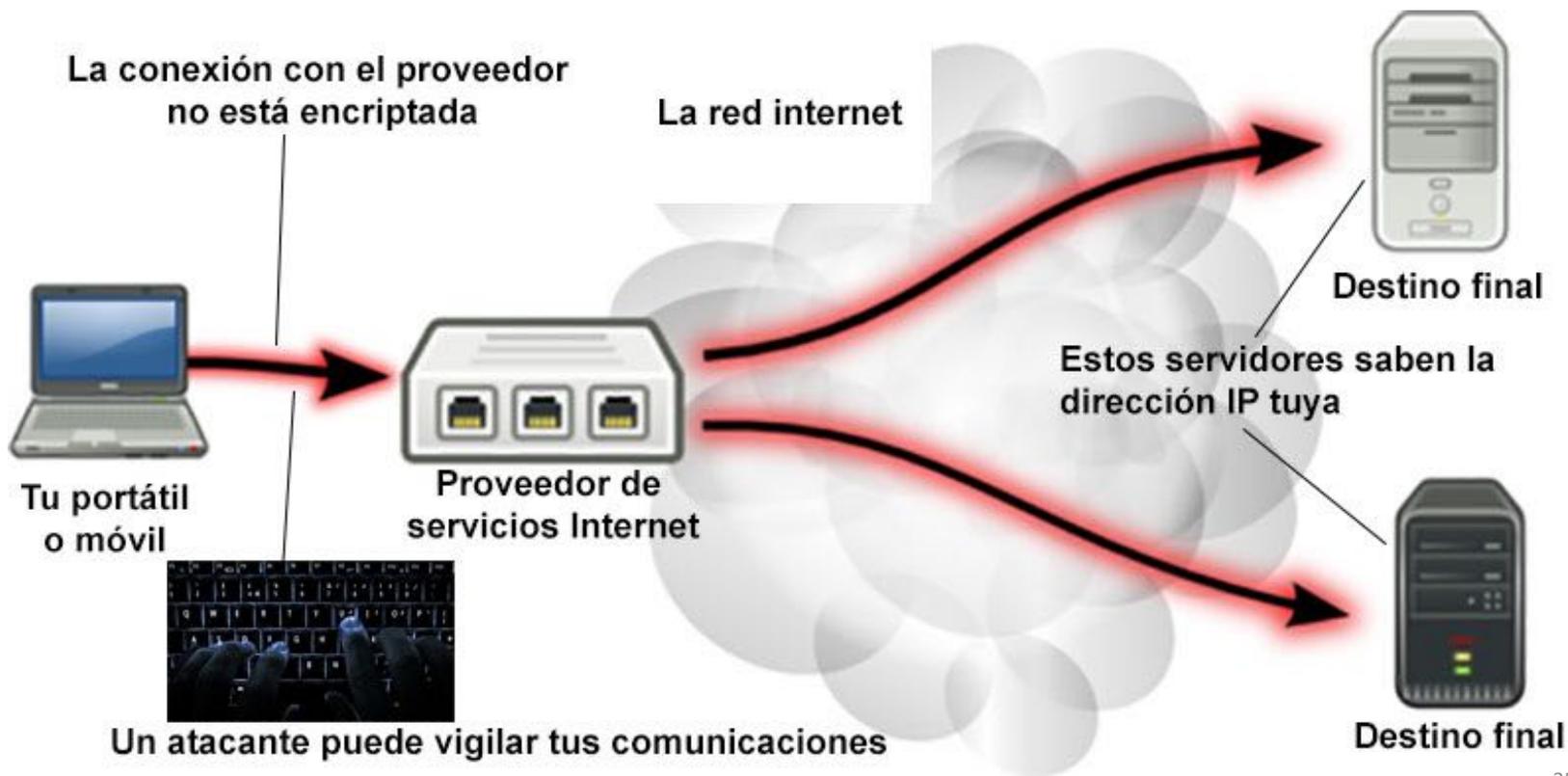
¿Preguntas?

Herramientas

Redes privadas virtuales

- Un ataque de intermediario pasa cuando hay una entidad entre tú y el sitio web, el servicio en línea o la persona con quien comunicas y esta entidad (el intermediario) es capaz de observar, interceptar, leer y hasta modificar la señal de comunicación.
- ¿Cómo arregla el intermediario obtener esta capacidad? Un método muy común es comprometerse una red WiFi (red inalámbrica).
- La herramienta para bajar tu susceptibilidad a este ataque es algo que se llama una red privada virtual -- una RPV (con siglas en inglés VPN por “Virtual Private Network”).

Así es como conectas al Internet sin una RPV:

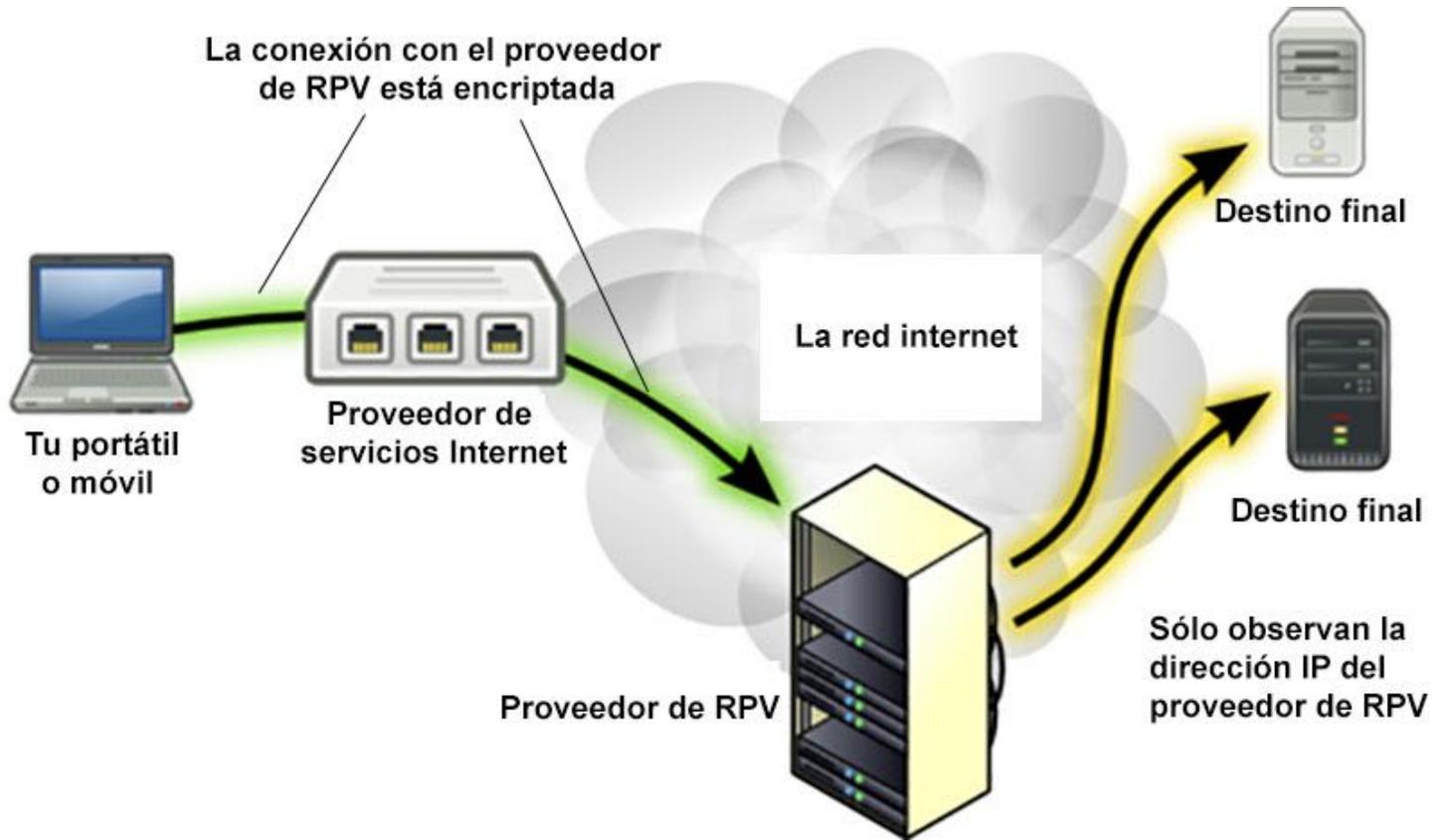


- Una RPV hace dos cosas:
 - Encripta tus comunicaciones digitales y por eso un atacante no puede vigilar tu actividad.
 - Entrega tus comunicaciones hasta un enrutador controlado por el proveedor de servicio de RPV, donde están enviadas hacia el destino final.

Y entonces, el destino final – Facebook.com, por ejemplo – cree que tu dirección IP es la del proveedor, y no la tuya verdadera dirección. Una RPV obscura tu verdadera dirección.

- Muchas RPV tienen enrutadores en docenas de países y permiten uno escoger de que país va a salir las comunicaciones hacia el internet público y entonces de que país estás supuestamente ubicado.

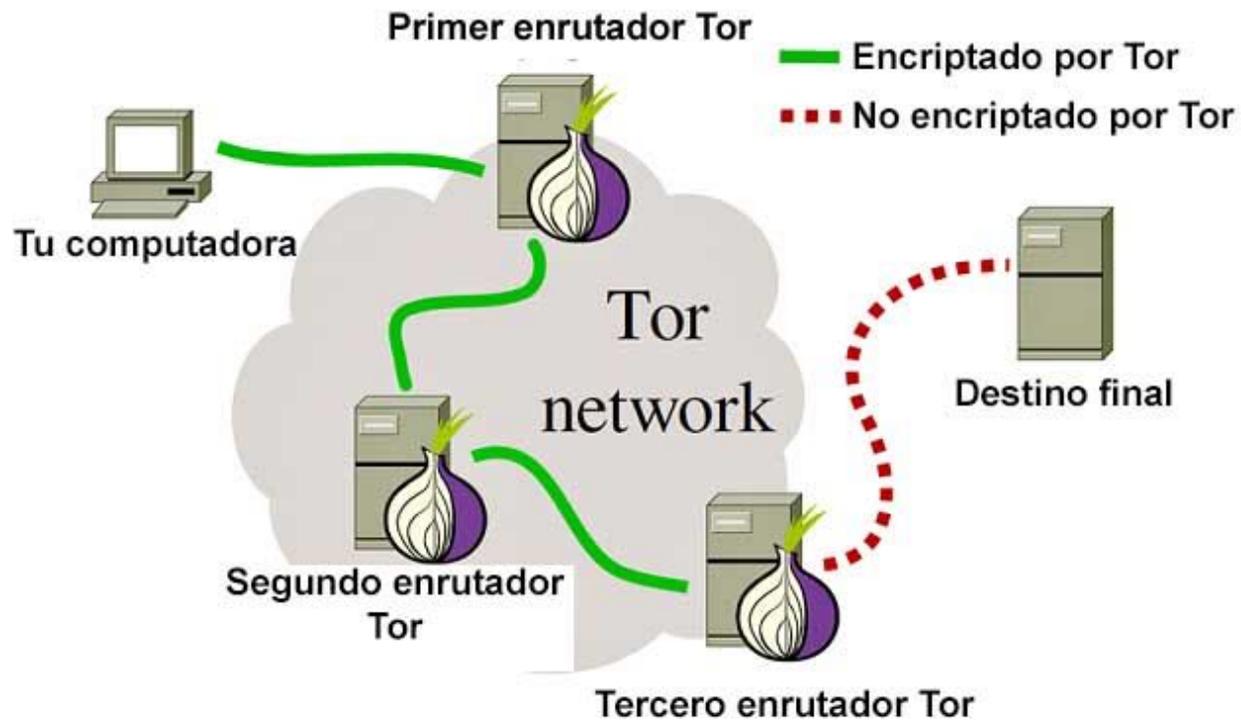
Así es como conectas al Internet con una RPV:



- Utiliza una RPV en todos tus dispositivos – el portátil, el móvil, todo lo que tienes.
- La RPV debe estar siempre activada.
- RPVs tiene una fuerte debilidad y es que el proveedor sabe todo lo que estás tratando de ocultar – tu dirección IP verdadera, los sitios web que visitas, los servicios en líneas que utilizas.
- Escoge un proveedor confiable. Una pregunta clave, es ¿en qué país está basado la firma? Porque el proveedor está sujeto a las leyes de ese país.
- Hay algunas RPVs gratuitas, pero pocas que son confiables:
 - PrivateTunnel (gratuito hasta 2 GB/mes) <https://www.privatetunnel.com>
 - TunnelBear (gratuito hasta 500 MB/mes) <https://www.tunnelbear.com/>
- Estés enlaces tienes listas de RPVs recomendados (en inglés)
 - <https://torrentfreak.com/vpn-anonymous-review-160220/>
 - <https://www.privacytools.io/#vpn>
 - <https://www.deepdotweb.com/vpn-comparison-chart/>

Como navegar por la web en forma anónima

- Existe otra herramienta para ocultar actividades en línea que funciona en una manera distinta de una RPV y pone más atención en conservar el anonimato que una RPV.
- Se llama Tor por sus siglas en inglés: The Onion Router (enrutador de cebolla)
- El logo de Tor es una cebolla porque las cebollas están hechas por capas distintas.
- Tor es una red hecha de enrutadores controlados por voluntarios.
- Todo el tráfico digital que pasa a través de Tor está se encamina encriptado por tres enrutadores y luego hacía el destino final.
- El tráfico llega a la red encriptado y mientras esté dentro de la red, permanece encriptado, y por eso muy difícil (hasta imposible) que el destino final sepa tu dirección IP verdadera. El punto débil de una RPV es que el proveedor puede observar tus actividades en línea, mientras en Tor tienes anonimato casi total.



- La herramienta normal para entrar la red Tor es un navegador hecho por el Tor Project, que es una organización sin ánimo de lucro en Boston.
- El navegador se llama “Tor Browser” y está disponible aquí:
<https://www.torproject.org/projects/torbrowser.html.en>
- En cambio de una RPV, Tor Browser funciona solamente cuando lo usas. Y Tor Browser no puede estar siempre encendido como una RPV debe de estar.
- Y sin duda, navegar el web por Tor Browser es más lento que otros navegadores. Además, algunos sitios bloquean tráfico con origen Tor o demandan constantemente que rellenes formularios Captcha.

- Tor sirve mejor como herramienta para evadir la censura en línea o vigilancia fuerte. Y si verdaderamente estás en peligro porque alguien peligroso te vigila, hay que tomar medidas avanzadas para mantener la privacidad con Tor.
 - En el Tor Browser, desactiva JavaScript, que está activado por defecto. También es buen consejo por los navegadores comunes, pero es difícil aguantar por mucho tiempo, porque sin JavaScript, casi todos los sitios web no funcionan.
 - Utiliza un “bridge” (un puente) para conectarse con la red Tor. Un puente hacia Tor es un relé para que entres en la red en forma más segura para que el proveedor de servicios Internet no pueda observar que estás conectada en Tor.
- Para leer más:
 - <https://ssd.eff.org/es/module/c%C3%B3mo-usar-tor-en-windows>
 - <http://es.gizmodo.com/que-es-tor-y-por-que-tu-tambien-deberias-usarlo-1591372289>

Y sobre puentes de Tor:

<http://lamiradadelreplicante.com/2013/12/30/evita-las-restricciones-de-tu-isp-a-la-red-tor-utilizando-bridges/>

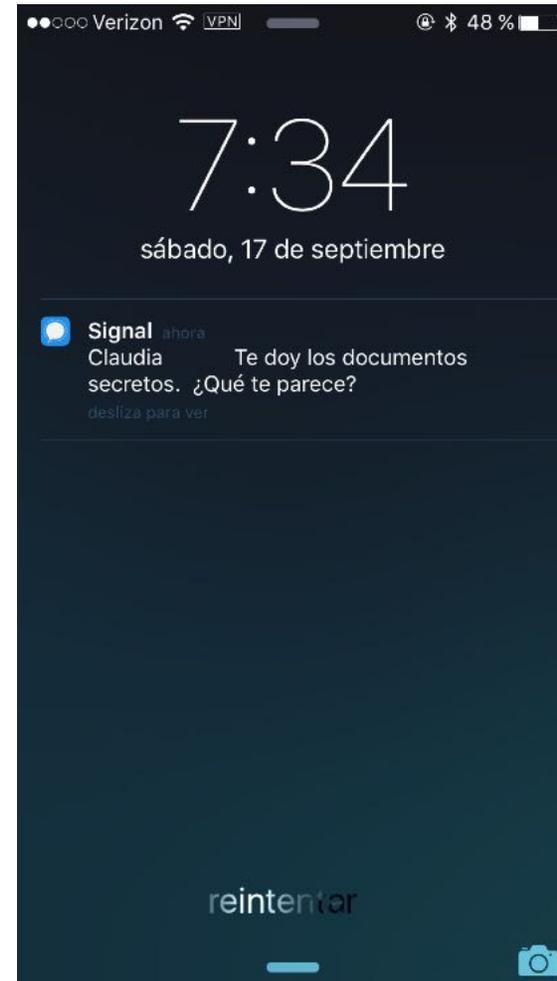
Proteger llamadas de voz y chat

- Un móvil siempre transmite una señal hasta las torres móviles y se conecta con la torre más cercana que tiene la más disponible ancho de banda.
- Hay tecnología que engaña un móvil a conectarse con una torre falsa con el propósito de localizar la ubicación de usuario, escuchar su conversaciones y leer su mensajes. Esta tecnología es conocida coloquialmente como un “Stingray” pero su nombre técnico es “IMSI catcher.”
- No hay manera de prevenir que tu móvil transmita esta señal de localización o una manera de confianza para prevenir que tu móvil se conecte con un Stingray si hay uno en los alrededores.
- Pero se puede prevenir a otros escuchar a escondidas digitalmente tus comunicaciones, con aplicaciones que las encriptan.

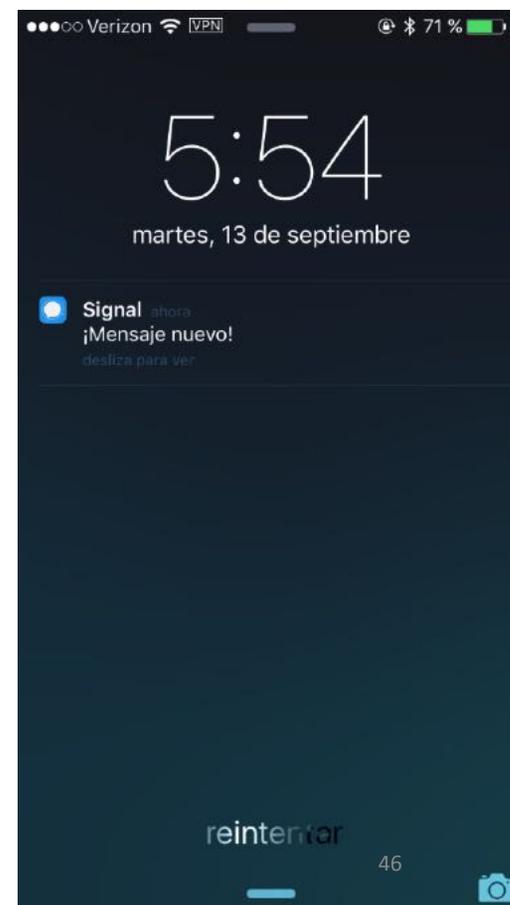
Signal

- La mejor aplicación es gratuita y de código abierto: **Signal**
- Está hecha por Open Whisper Systems, una organización sin ánimo de lucro fundada por activistas digitales en San Francisco.
- Con Signal, puedes chatear, hacer llamadas de voz y mensajes multimedia.
- Signal ofrece por defecto encriptación punto a punto – las claves quedan en tu móvil, fuera del control de un tercero (incluyendo Open Whisper Systems).
- Puedes chatear en manera segura (encriptada) con un grupo, no solo con una persona a la vez.
- Signal está disponible para iPhone y Android.

- Ojo: Si te comunicas con gente sensible a través de Signal, configura la app para que el nombre del remitente y la vista previa del mensaje no salgan en la pantalla bloqueada. Hay que evitar algo como el ejemplo a la derecha, especialmente si has perdido tu móvil o alguien te está vigilando.
- De hecho, mejor configurar el móvil para ningún mensaje de chat o correo electrónico muestre el remitente o la vista previa en la pantalla bloqueada. Consulta el Apéndice C (iPhone) o Apéndice D (Android) para leer más.



Como ajustar notificaciones de Signal por iPhone para ocultar la identidad del remitente



Como ajustar notificaciones de Signal por Android para ocultar la identidad del remitente:

- Las diferentes marcas de Android ponen la menú de configuraciones en lugares distintos, pero generalmente:
 - Abre Ajustes
 - Toca Notificaciones
 - Quizás primero hay que tocar Avanzados
 - Toca En la pantalla bloqueada a continuación: Ocultar notificaciones sensibles.
 - Hay otra opción de “No mostrar notificaciones,” pero si la escoges, será difícil saber cuando alguien te está comunicado a través de Signal.
- Si llevas un Android viejo, el sistema operativo quizás no tiene opción de ocultar notificaciones en la pantalla bloqueada.
- Este artículo tiene aún más consejo en como utilizar Signal seguramente (pero es en Inglés)
<https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/>

- Open Whisper Systems está en proceso de desarrollar una versión para las computadoras de escritorio y portátiles y desde April una versión “beta” está disponible para el público para el uso con navegadores de Google Chrome.
- Para leer más de otra opciones que existen para la llamadas y chat seguros, consulta Apéndice B de esta presentación.

Enlace para Open Whisper Systems: <https://whispersystems.org/>

Descarga Signal

- iPhone: <https://itunes.apple.com/us/app/signal-private-messenger/id874139669>
- Android:
https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&referrer=utm_source%3DOWS%26utm_medium%3DWeb%26utm_campaign%3DNav

Leer más sobre Signal para computadoras aquí: <https://whispersystems.org/blog/signal-desktop-public/>

Encriptar y fortalecer tus dispositivos

- Los datos existen en dos formas básicas:
 - cuando están en marcha por una red (la transmisión), y
 - cuando se quedan en el almacenamiento (o como se dice en inglés, cuando “los datos descansan”).
- La sección anterior se trató de datos en vez de transmisión. Hablamos ahora de cómo proteger los datos almacenamientos.
- ¿Para qué sirve datos almacenamientos cifrados? Aunque sea contrario a la intuición, es mayormente por cuando te desconectes de tu computadora o apagues tu móvil.
- ¿Entonces, por qué es útil la encriptación? Porque cuando pierdes el móvil o el dispositivo USB o cuando te roben el portátil, no pueden ganar acceso a tus datos.

Encriptar y fortalecer tus dispositivos: iPhone

- Los iPhones a partir de la versión del sistema operativo iOS 8 (que salió al mercado en 2014) están cifrados de forma predeterminadamente.
- El más antiguo iPhone que tiene compatibilidad con iOS 8 es iPhone 4S.
- Entonces, si tienes iPhone 4S o un modelo más nuevo y has actualizado el sistema operativo a lo más reciente, no tienes que hacer nada para encender la encriptación, y está.
- A pesar de este, hay medidas para aumentar la seguridad aún más.
- Consulta Apéndice C de esta presentación para aprender más.

Encriptar y fortalecer tus dispositivos: Android

- El sistema operativo Android ofrece más complicaciones que los iPhones, porque en contraste con Apple, la misma compañía no siempre controla el sistema operativo y el hardware. El sistema operativo está hecho por Google y varias empresas de calidad variable fabrican los móviles.
- Móviles que llevan la marca “Nexus” como “Galaxy Nexus” de Samsung están hechos con colaboración cercana entre el fabricante y Google, y por eso tienen una calidad garantizada.
- Por ejemplo, móviles Nexus son generalmente los primeros para recibir actualizaciones de firmware.
- Particularmente por las actualizaciones, desde el punto de vista de seguridad, el consejo de expertos es comprar un modelo Nexus.
- Los dispositivos Nexus 5X, Nexus 6P, Nexus 6 y Nexus 9 están encriptados de forma predeterminada.
- Consulta Apéndice D de esta presentación para aprender más.

Encriptar y fortalecer tus dispositivos: dispositivos USB con VeraCrypt

- VeraCrypt es una gratuita y nueva variación de una aplicación de encriptación mantenida por voluntarios llamado TrueCrypt. En 2014, los voluntarios abruptamente dejó de mantenerla y por eso fue nacido VeraCrypt, mantenido por un nuevo grupo.
- No es VeraCrypt necesariamente la mejor solución para encriptar discos duros enteramente, pero para dispositivos USB, funciona muy bien.
- Consulta Apéndice F para instrucciones.
- Puedes también consultar este sitio web:
<http://www.blogdeizquierda.com/2015/05/mundo-bitcoin-como-encriptar-un-usb.html>

Encriptar y fortalecer tus dispositivos: contenedores en tu disco duro o en la nube con VeraCrypt

- Un contenedor encriptado es una carpeta virtual donde puedes almacenar encriptadamente archivos sensibles.
- Es mejor encriptar toda tu computadora, pero VeraCrypt puede ofrecer complicaciones en este objetivo. Como encriptar un disco duro entero es el tema siguiente.
- Si no puedes encriptar toda el disco duro o quieres almacenar archivos en la computación de la nube, VeraCrypt sigue siendo una buena opción.
- Si utilizas un servicio de computación en la nube como DropBox o Google Drive para almacenar archivos sensibles, encriptalos con VeraCrypt antes de subirlos a la nube.
- Consulta Apéndice G para instrucciones.

Encriptar y fortalecer tus dispositivos: Windows

BitLocker

- BitLocker es una aplicación de encriptación hecha por Microsoft. Si tu computadora funciona con sistema operativo Microsoft, es probablemente la mejor opción.
- Con BitLocker, conservas el control sobre la encriptación, en contraste con otras formas de encriptación que Microsoft ofrece.
- Existen algunos quienes están escéptica de Microsoft porque sospechan que la firma haya dejado una puerta trasera que solo conoce la Agencia de Seguridad Nacional de los EE.UU (NSA por las siglas in inglés). Si es verdad, NSA podrá desencriptar cualquiera computadora.

- Examinamos la hipótesis. Microsoft ha fuertemente negado que existe una puerta trasera (por supuesto, se diría este aunque si fuera mentira o verdad).
- Pero tecnólogos independientes han escrito que parece que Bitlocker está seguro. (Puedes ver un artículo en inglés aquí: <https://theintercept.com/2015/06/04/microsoft-disk-encryption/>)
- Y vamos al modelo de riesgos: ¿Estás amenazado por el riesgo que la NSA robe tu computadora?
- Vea el Apéndice F para aprender más de otras métodos en encriptar una computadora Windows.
- Vea Apéndice G y H de esta presentación para aprender más sobre como utilizar BitLocker.

Encriptar y fortalecer tus dispositivos: Mac

- Como suele ser, Apple ofrece una opción sencilla para sus usuarios, al tiempo que asume que confías absolutamente en la empresa (algo que ni siquiera Microsoft hace).
- Instrucciones para encriptar los discos duros Mac están aquí : <https://support.apple.com/es-us/HT204837>
- Ojo, que Apple deja a usuarios cambiar la contraseña de la encriptación mediante la Identificación de una cuenta de Apple.

Almacenamiento seguro por la computación en la nube

- Hay proveedores de almacenamiento en la nube que se anuncian como un “proveedor de confianza y privacidad.”
- Por ejemplo, hay algunos que ofrecen encriptación punto-a-punto bajo la garantía de que ni siquiera ellos pueden acceder a tus archivos.
- Tresorit (<https://tresorit.com/>) es uno; SpiderOak es otro (<https://spideroak.com/>).
- Pero la mejor opción es encriptar por sí mismo archivos sensibles antes de subirlos a cualquier proveedor de computación en la nube.
- Al fin del día, tú y sólo tú eres responsable para mantener la confianza de fuentes de información y de guardar tus secretos
- Te refiero a la sección y los apéndices sobre encriptación. Con VeraCrypt, puedes crear un volumen encriptado directamente en la nube y guardar documentos en el volumen.



¿Preguntas?

Apéndice A: Autenticación de dos factores - ejemplo de Gmail

Google

Mi Cuenta

Te damos la bienvenida, David Perera

Controla, protege y asegura tu cuenta, todo en un solo lugar.

Mi cuenta te brinda acceso rápido a las opciones de configuración y las herramientas que te permiten proteger los datos y la privacidad. Además, puedes decidir de qué forma usar tu información para mejorar el funcionamiento de los servicios de Google.

Acceso y seguridad >

Información personal y privacidad >

Preferencias de la cuenta >

Controla la contraseña y la configuración de acceso a los datos de la cuenta.

Cómo acceder a Google

Notificaciones y actividad de dispositivos

Aplicaciones y sitios conectados

Administra la configuración de visibilidad y los datos que utilizamos para personalizar tu experiencia.

Tu información personal

Administrar tu actividad de Google

Configuración de anuncios

Configura el idioma, la accesibilidad y otras opciones de configuración que te permiten utilizar mejor Google.

Herramientas de captura de texto e idioma

Accesibilidad

Tu almacenamiento de Google Drive

59

Mi Cuenta

Te damos la bienvenida.

- Acceso y seguridad**
- Cómo acceder a Google
- Notificaciones y actividad de dispositivos
- Aplicaciones y sitios conectados

Acceso y seguridad

Nota: para modificar estas opciones de configuración, deberás confirmar la contraseña.

Contraseña	Última modificación: 5 de agosto de 2012	>
Verificación en dos pasos	Desactivada	>



Configurar el teléfono

¿Qué número de teléfono deseas usar?

Google solo usará este número como método de seguridad de la cuenta.
No ingreses un número de Google Voice.
Se pueden aplicar cargos por mensajes y datos.

¿Cómo deseas obtener los códigos?

- Mensaje de texto Llamada telefónica

Paso 1 de 3

[PROBAR](#)



Confirma que funciona

Google acaba de enviar un mensaje de texto con un código de verificación al **(703) 946-2556**.

Ingresar el código

¿No lo recibiste? [Volver a enviar](#)

[ATRÁS](#)

Paso 2 de 3

[SIGUIENTE](#)

← Verificación en dos pasos

Tu segundo paso

Después de ingresar tu contraseña, se te pedirá que realices un segundo paso de verificación. [Más información](#)



Mensaje de texto o de voz (Predeterminado) ?

(703) 946-2556

Los códigos de verificación se envían por mensaje de texto



Configurar un segundo paso alternativo

Configura al menos una opción alternativa para que puedas acceder, incluso si no tienes el teléfono a mano.



Códigos de copia de seguridad

Estas contraseñas de uso único y para imprimir te permiten acceder a tu cuenta cuando no tienes tu teléfono a mano, por ejemplo, si estás de viaje.

[CONFIGURACIÓN](#)



Avisos de Google

Recibe un mensaje de Google en tu teléfono y presiona **Sí** para acceder.

[AGREGAR TELÉFONO](#)



App del Autenticador

Usa la app del Autenticador para obtener códigos de verificación gratuitos, incluso cuando el teléfono esté sin conexión. Disponible para Android y iPhone.

[CONFIGURACIÓN](#)

← Verificación en dos pasos

tu segundo paso

Después de ingresar tu contraseña, se te pedirá que realices un segundo paso de verificación. [Más información](#)



Obtener los códigos a través de la app del Autenticador

En lugar de esperar la llegada de mensajes de texto, obtén códigos de verificación de forma gratuita desde la app del Autenticador. Funciona incluso si el teléfono está sin conexión.

¿Qué tipo de teléfono tienes?

Android

iPhone

[CANCELAR](#) [SIGUIENTE](#)

Configurar un

Configura al m
mano.



App del Autenticador

Usa la app del Autenticador para obtener códigos de verificación gratuitos, incluso cuando el

← Verificación en dos pasos

Tu segundo paso

Después de ingresar tu contraseña, se te pedirá que realices un segundo paso de verificación. [Más información](#)



Se configuró el Autenticador.

- Descarga la app del Autenticador en la [App Store](#).
- En la app, selecciona **Configurar cuenta**.
- Selecciona **Escanear código de barras**.



[¿NO SE PUEDE ESCANEAR?](#)

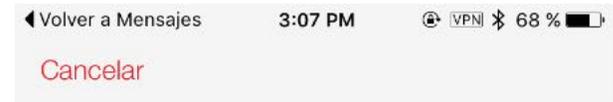
[CANCELAR](#) [SIGUIENTE](#)



App del Autenticador

Usa la app del Autenticador para obtener códigos de verificación gratuitos, incluso cuando el teléfono esté sin conexión. Disponible para Android y iPhone.

- Descarga Google Authenticator o Authy y agrega cuenta
- La app va a pedir permiso para acceder a la cámara de móvil
- Con la cámara, tomo una foto del código QR en la pantalla



Agregar Cuenta

Tu puedes agregar cualquier cuenta que use Google Authenticator tales como Gmail, Facebook, Dropbox, Evernote y muchas más usando authy.

Las cuentas se agregan escanando un código QR o ingresando manualmente una llave que se obtiene del sitio web correspondiente. [Toca aquí para aprender más.](#)



Escánear código QR

[Ingresa la llave manualmente.](#)

- La app **no** debe ser Google Authenticator
- Puedes utilizar cualquier app de autenticación de dos factores – como Authy
- Al final, cada vez que inicias sesión en tu cuenta de Google, necesitarás tu móvil para ingresar un código de verificación.



El token de [redacted]@gma... es:

613 108

El token expira en 15



 Google stan.krun@gm...	 Agregar Cuenta
--	---



2-Step Verification

Para ayudarte a proteger tu correo electrónico, fotos y demás contenido, completa la tarea que aparece a continuación.



Ingresa un código de verificación

Obtener un código de verificación de la app del **Autenticador de Google**

Ingresa el código de 6 dígitos

Finalizado

No volver a preguntar en esta computadora

Te sugerimos que mantengas esta opción seleccionada. En los dispositivos compartidos, se recomienda tomar precauciones adicionales. [Más información](#)

Apéndice B: Otras aplicaciones para llamadas de voz y chat seguros

Wickr

Chateo, pero puedes enviar mensajes de voz y compartir archivos de manera segura. Wickr tiene la desventaja de las conversaciones pasan por sus servidores. Pero, a la misma vez, las conversaciones están cifradas punto-a-punto y Wickr tiene la ventaja de que los mensajes desaparezca de los dos dispositivos (él que lo envió y él que lo recibió) luego de una cantidad de tiempo, desde unos minutos hasta días. Hay versiones para el móvil y para la computadora.

<https://www.wickr.com/>

WhatsApp

Llamadas, chateo y el intercambio de archivos (no más largos que 100 MB). La versión más reciente de WhatsApp ofrece encriptación punto-a-punto siempre activada y un método para confirmar que el cifrado está activado. Hay versiones para el móvil y para la computadora.

WhatsApp tiene la desventaja de las conversaciones pasan por sus servidores y entonces hay la posibilidad de que conserva metadatos sobre de quien está comunicando con quien.

Por defecto, WhatsApp almacena mensajes para que el servicio de copia de seguridad automática de iPhone o Android los copia. Entonces, Apple (iPhone) o Google (Android) pueden tener copias de sus mensajes. Otra vez, hay que preguntarse si este hecho vale como un riesgo debajo tu modelo de riesgos.

<https://www.whatsapp.com/>

<https://www.whatsapp.com/faq/es/general/28030015>

<https://www.whatsapp.com/faq/es/web/26000010>

OTR

“Off the record” (“fuera del registro” por la siglas en inglés) es un protocolo para chateo cifrado punto-a-punto mayormente utilizando en combinación de Pidgin, una aplicación de mensajería instantánea para las computadoras.

Los dos – OTR y Pidgin – son de código abierto y son gratuitos.

Una desventaja es mensajes están encriptados solo cuando comuniqués con una sola otra persona – el chateo de grupo está encriptado.

Hay que configurar Pidgin antes de utilizarlo.

Instrucciones para Windows: <https://ssd.eff.org/es/module/como-usar-otr-en-windows>

Instrucciones para Mac: <https://ssd.eff.org/es/module/c%C3%B3mo-usar-otr-para-mac>

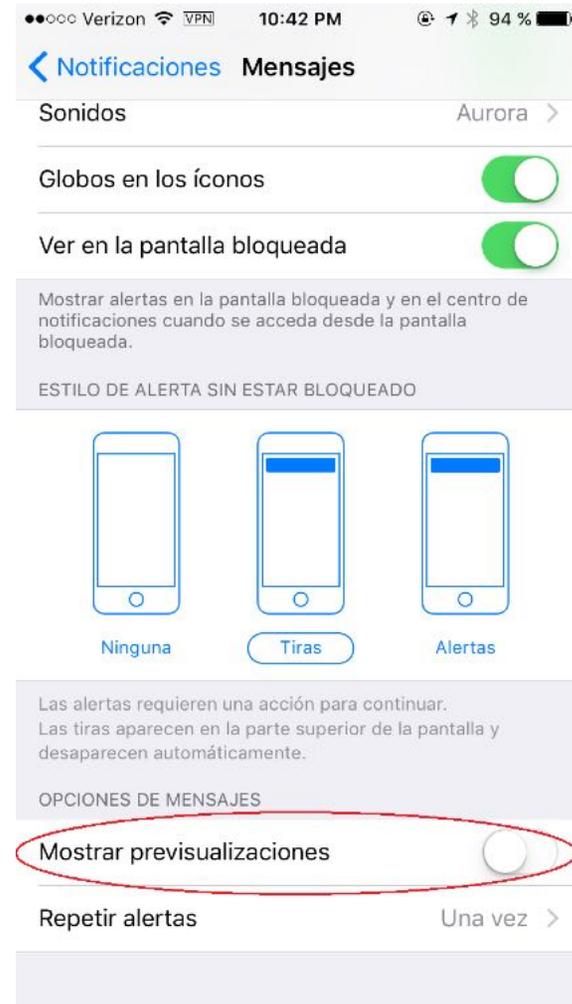
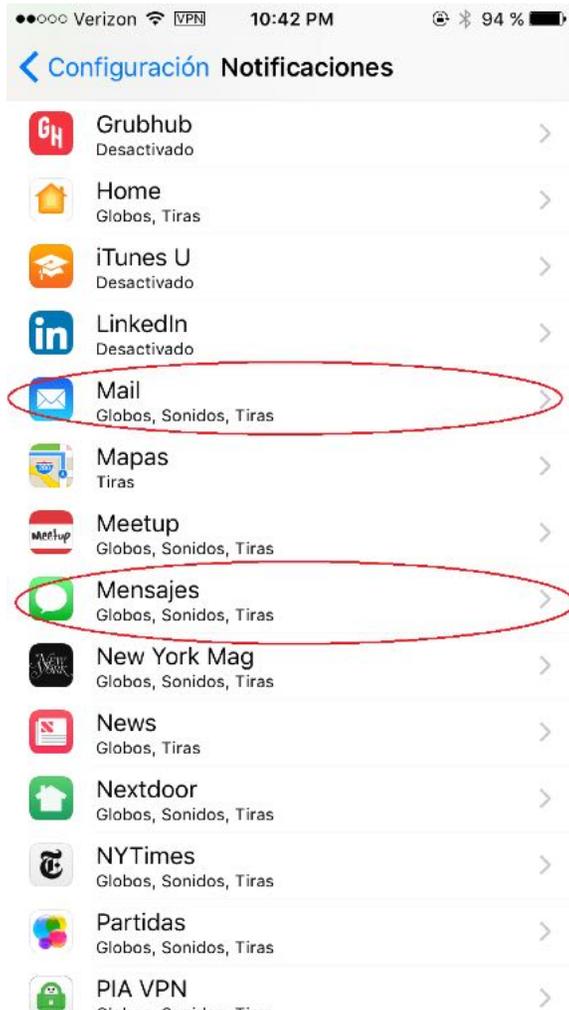
Telegram

Hay dudas sobre la seguridad de Telegram, y tiene el problema que no cifra mensajes de forma predeterminada. Tienes que activar el cifrado. Este automáticamente te pone en más riesgo que es necesario, porque un día puedes olvidar hacerlo o quizás llega el día en que piensas que el cifrado está activada pero no lo está.

Apéndice C: Medidas para iPhones

- Elige un código de al menos siete números para desbloquear el iPhone. Puedes cambiar el código así:
Configuración → Touch ID y código
Apague la opción para “código sencillo.”
- Debes configurar la opción “Solicitar” para “De inmediato”, para que tu dispositivo no sea desbloqueado cuándo no le estés utilizando.
Bloquea el “código sencillo” para poder utilizar un código con más de 4 dígitos.
- Al fondo de la pantalla, verifica que hay esta frase: “La protección de datos está activado”
- También, verifica que has escogido la opción “Borrar datos.” Si sí, todos los datos en el iPhone se borran después de 10 intentos fallidos de ingresar el código.
- Con la combinación de un código fuerte más de siete números y la opción de borrar datos, es casi imposible que alguien tenga acceso al iPhone tuyo sin tu conocimiento.

- Escoge un bloqueo automático de poco tiempo así si no lo utilizas activamente, el iPhone se cierra la pantalla. Si lo puedes aguantar, escoge 1 minuto; si no, 2 minutos:
Configuración → General → Bloqueo automático
- Si comunicas con gente sensible por email configura el móvil para no mostrar previsualizaciones en la pantalla bloqueada: Configuración → Notificaciones → Mail
- Haz lo mismo con mensajes de texto (aunque es muy recomendable que uses Signal para chatear):
Configuración → Notificaciones → Mensajes



- Si sincronizas tu iPhone con iCloud, desde iOS 9.3 puedes proteger la copia backup almacenado por Apple con un código.
- Si sincronizas tu iPhone con iTunes y dejas copias de tu iPhone en la computadora, selecciona la opción “Encriptar backup” a la lanqueta “Summary”.
- Puedes también configurar tu dispositivo Apple para ser formatado remotamente, utilizando la función “Find My iPhone” por si acaso que lo pierdes. A la vez, esto permitirá a Apple localizar remotamente su dispositivo a cualquier momento. Debes equilibrar los beneficios de borrar datos caso per caso pierdes control de su dispositivo, bajo el riesgo de revelar su posición a Apple. ¿Para te, cual es el riesgo más fuerte?
- Lea más aquí: <https://ssd.eff.org/es/module/c%C3%B3mo-encriptar-su-iphone>

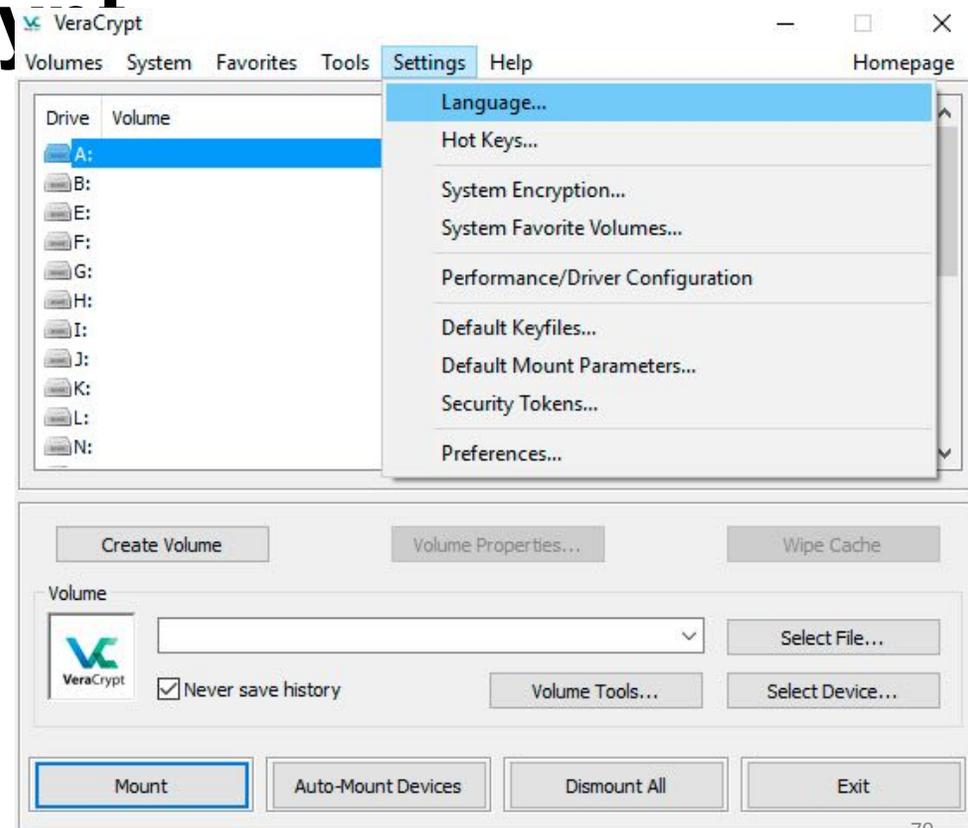
Apéndice D: Medidas para Android

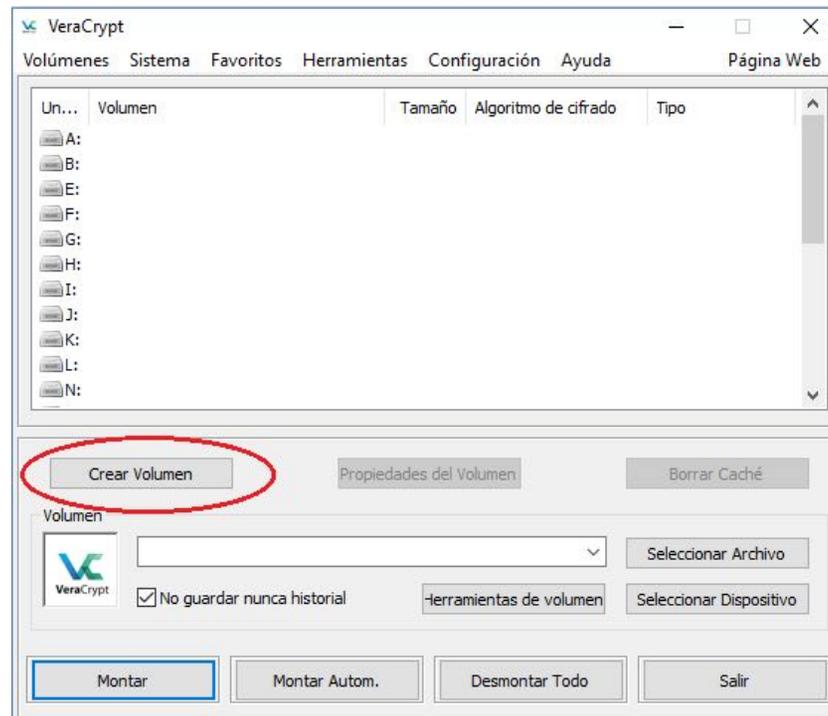
- La política de Google es proporcionar actualizaciones para modelos de Android con marca Nexus por lo menos tres años desde cuando un nuevo modelo Nexus sale al mercado, o por lo menos 18 meses desde cuando el último modelo de una versión nueva está vendido, cualquiera periodo sea más larga.
- Los dispositivos Nexus 5X, Nexus 6P, Nexus 6 y Nexus 9 están cifrados de forma predeterminada.
- Nexus 4, Nexus 5, Nexus 7 y Nexus 10 (la última es una tableta, no un móvil) no están encriptados de forma predeterminada, pero tienen la capacidad para quedar encriptados. Según Google, el proceso encriptación para estos dispositivos tarda aproximadamente una hora.
- Si tienes un móvil Android que está viejo o tiene una capacidad de memoria o computación baja, es posible que la encriptación se ralentizará el móvil. Y una vez hecho, la encriptación *es imposible deshacer sin el perdido total de tus datos*.
- Instrucciones para cifrar dispositivos Nexus está aquí:
<https://support.google.com/nexus/answer/2844831?hl=es>

- Si todavía no tienes un bloqueo de pantalla, configura el móvil para que lo tenga. Instrucciones que valen para dispositivos de Android 7 (que salió muy recientemente al mercado) está aquí:
<https://support.google.com/nexus/answer/2819522?hl=es>
- Otras medidas para la seguridad:
 - Descargar aplicaciones solo desde Google Play.
 - Si tienes tienda de aplicaciones que no es de Google, bórrala.
 - Solo utilizar Chrome por el navegador, y siempre actualiza Chrome.
- Google tiene un sitio web con más información sobre ciberseguridad de Android aquí:
https://www.android.com/intl/es_es/security/overview/#

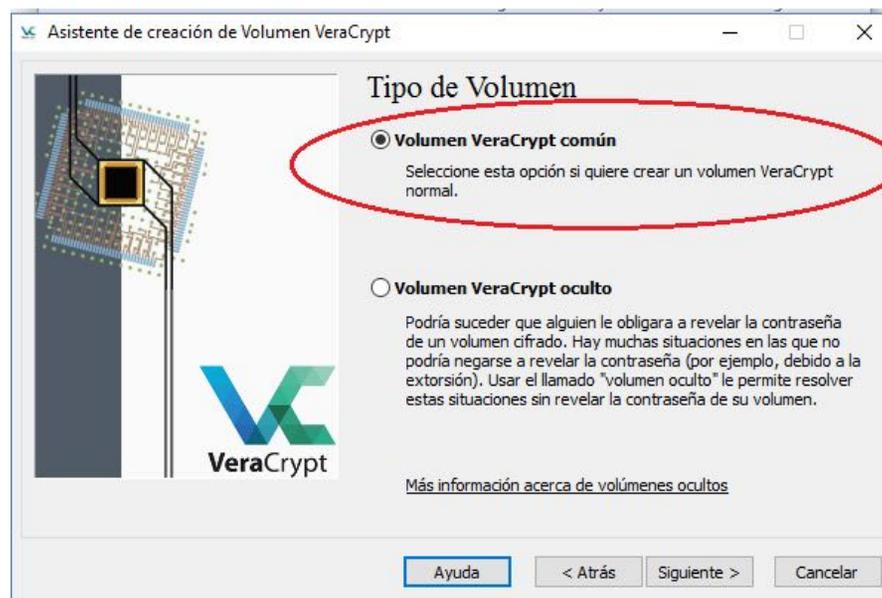
Apéndice F – Encriptando dispositivos USB con VeraCrypt

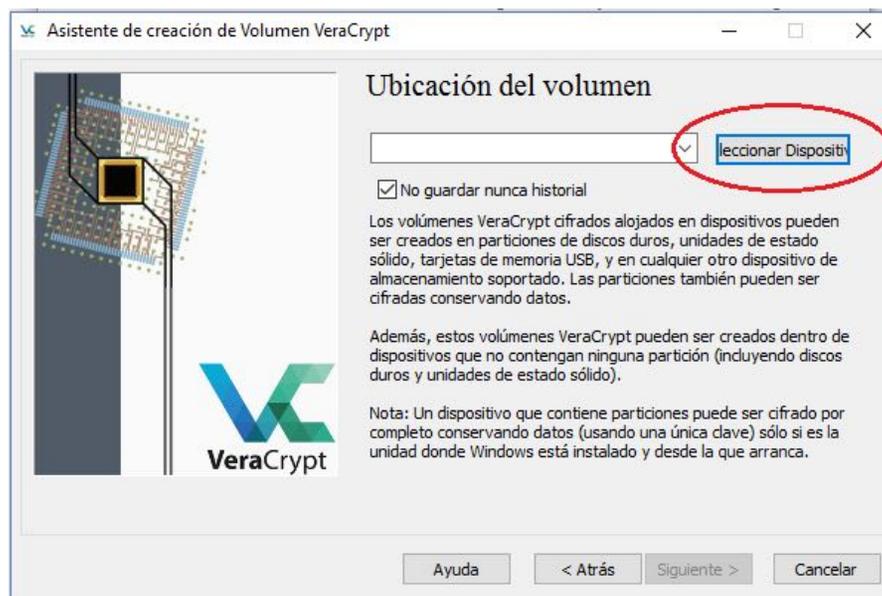
- Descarga VeraCrypt aquí:
<https://veracrypt.codeplex.com/>
- En este ejemplo, vamos con un dispositivo USB vacío, sin archivos
- Cambia el lenguaje a español haciendo clic sobre "Settings"



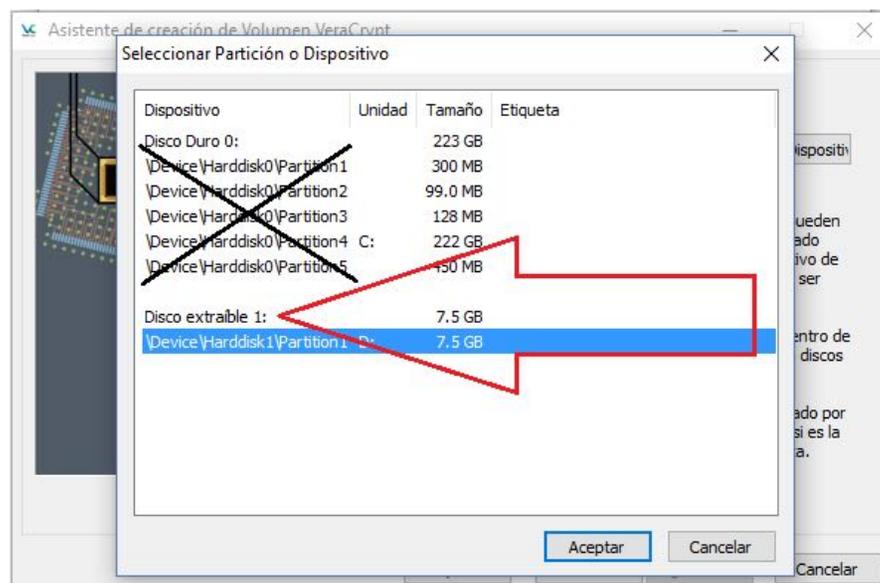








Ojo que escoges el disco extraíble (el dispositivo USB) y **no el disco duro**









Asistente de creación de Volumen VeraCrypt

Contraseña del Volumen

Contraseña:

Confirmar:

Usar archivo-llave

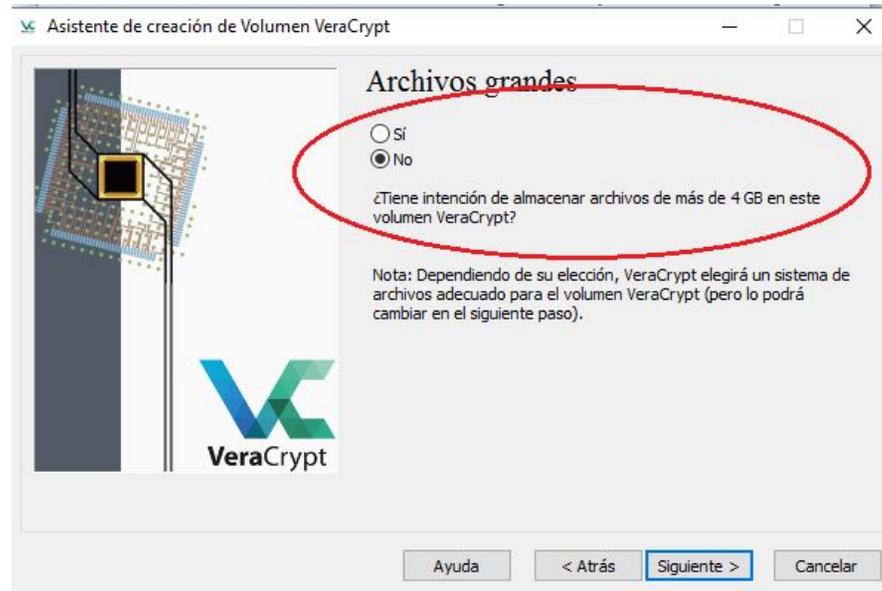
Mostrar contraseña

Use PIM

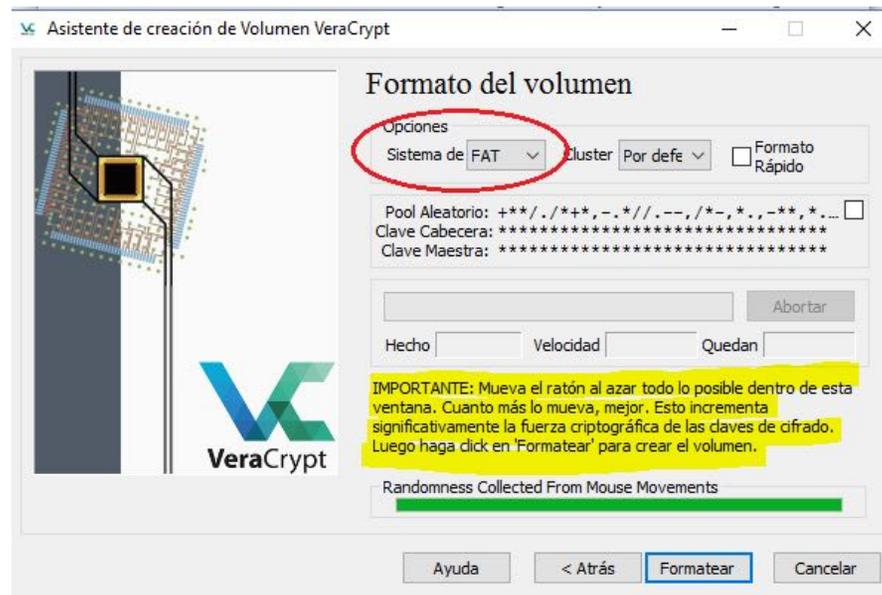
Es muy importante que elija una buena contraseña. Debería evitar elegir una que contenga sólo una palabra que se pueda encontrar en un diccionario (o una combinación de 2, 3, o 4 de estas palabras). No debería contener nombres ni fechas de nacimiento. No debería ser fácil de adivinar. Una buena contraseña es una combinación aleatoria de letras mayúsculas y minúsculas, números, y caracteres especiales como @ ^ = \$ * + etc. Recomendamos la elección de una contraseña que consista en más de 20 caracteres (cuanto más larga, mejor). La máxima longitud posible es 64 caracteres.

Ayuda < Atrás Siguiendo > Cancelar

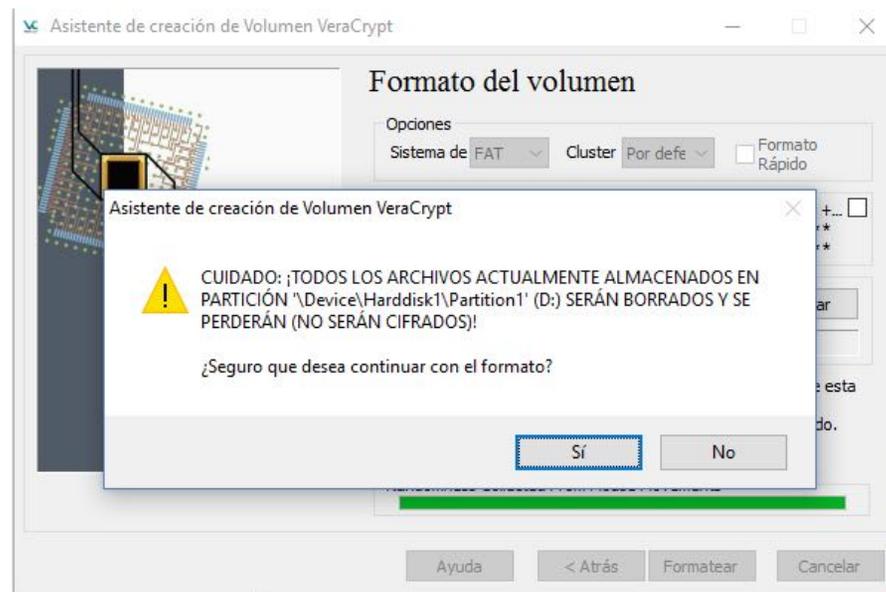
Si de veras vas a almacenar archivos más grande de 4 GB in el volumen encriptado, escoge “Sí.”
VeraCrypt funcionará mejor si escoges “No”.



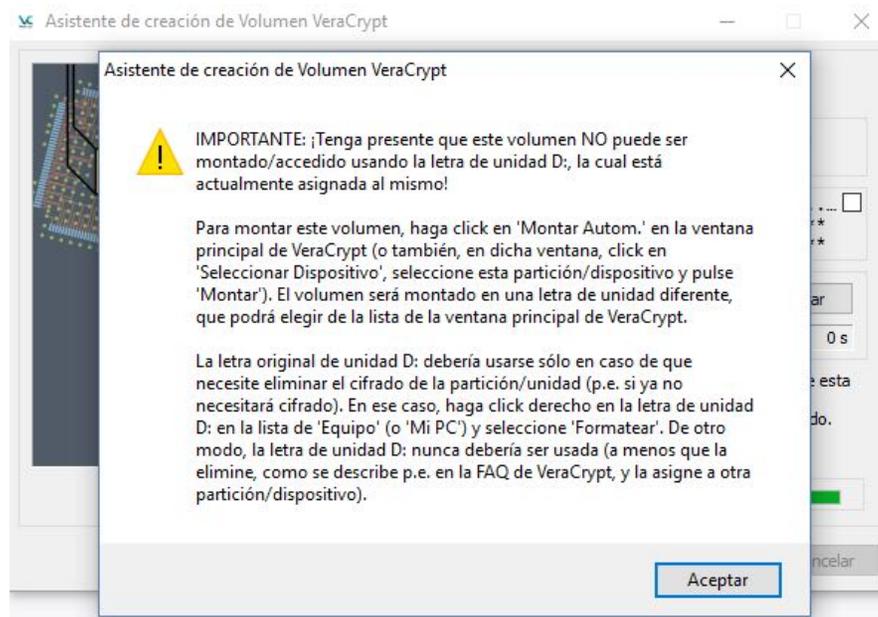
FAT es un sistema de archivos y es admitido prácticamente por todos los sistemas operativos existentes.



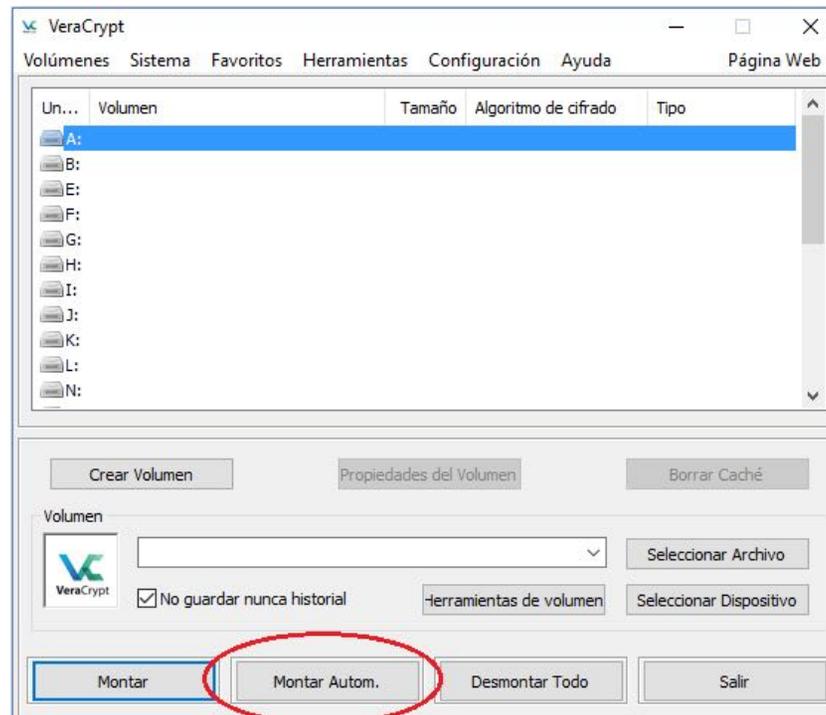
En esta etapa, mueve el ratón porque de esa manera Veracrypt genera números al azar para aumentar la fuerza criptográfica. No pares hasta que el indicador se vuelve verde.

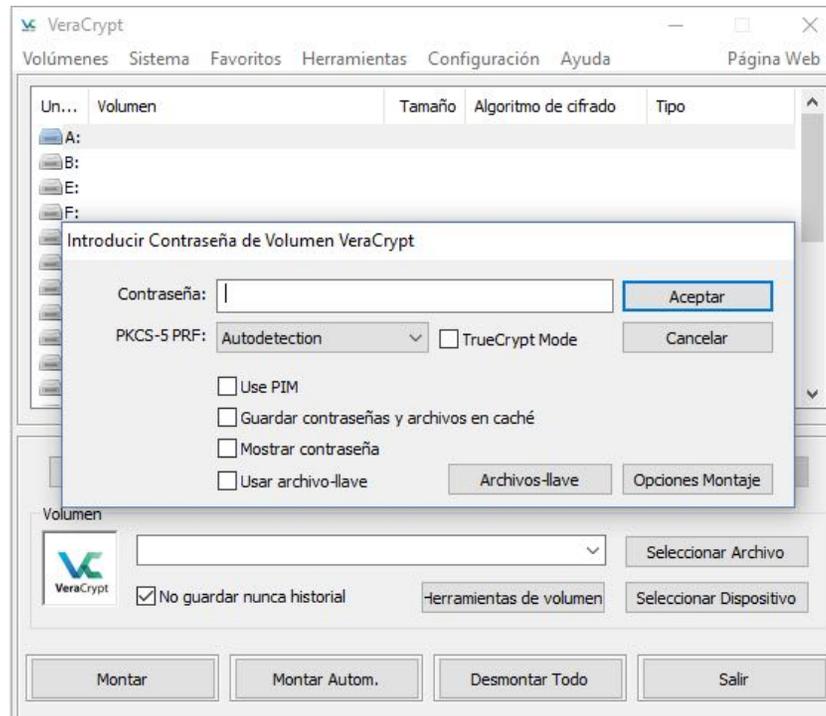




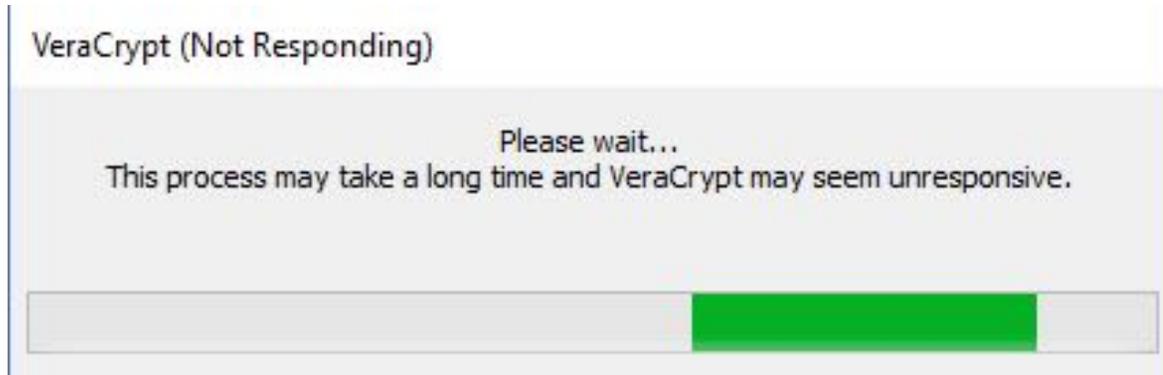


Para abrir tu dispositivo USB encriptado, haz clic in “Montar Automáticamente.”

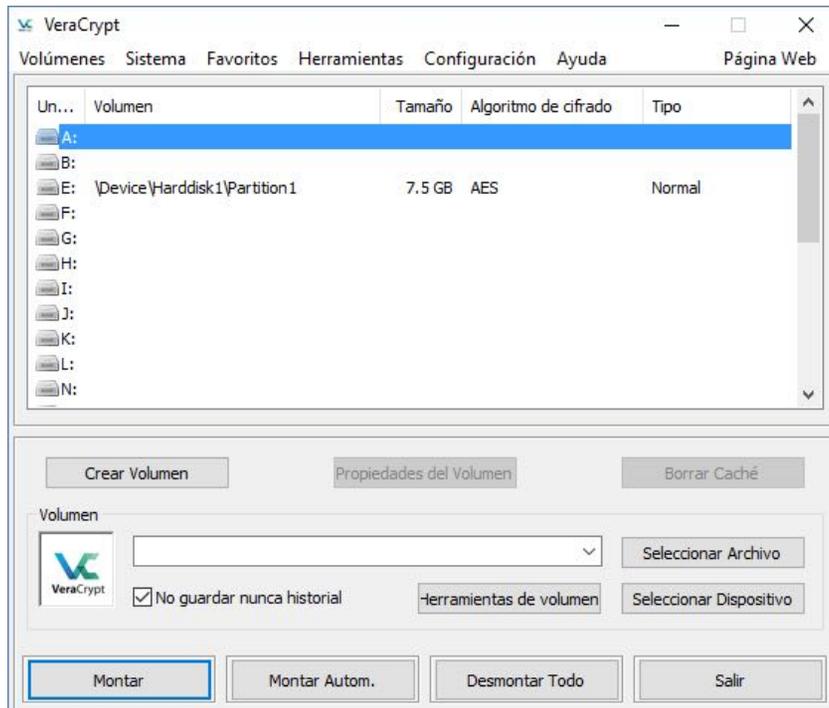




“Este proceso puede durar mucho tiempo y VeraCrypt no responderá a mandos”

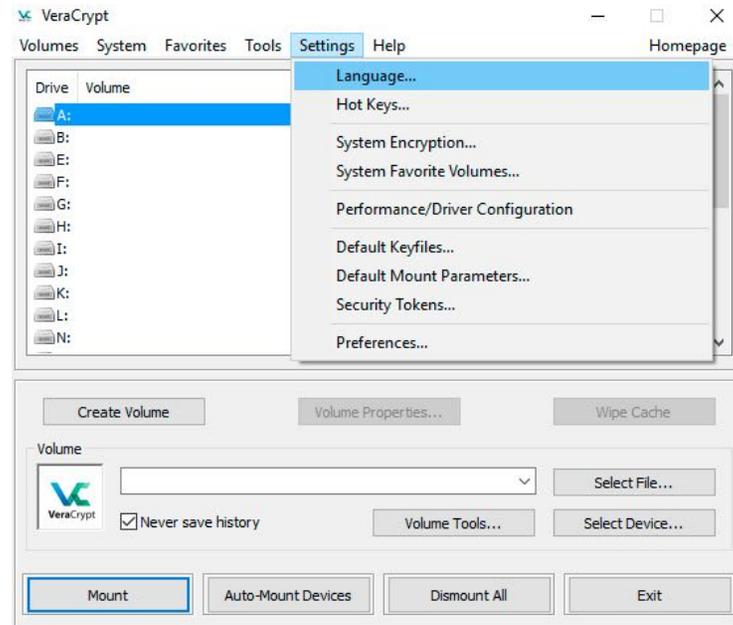


El este ejemplo, VeraCrypt ha montado el dispositivo USB encriptado como Volumen E. Haz clic dos veces al volumen y puedes guardar archivos al dispositivo.



Cuando estás terminado utilizando estos archivos, no te olvides desmontar el volumen.

Apéndice G – Encriptar y fortalecer tus dispositivos: contenedores en tu disco duro o en la nube con VeraCrypt





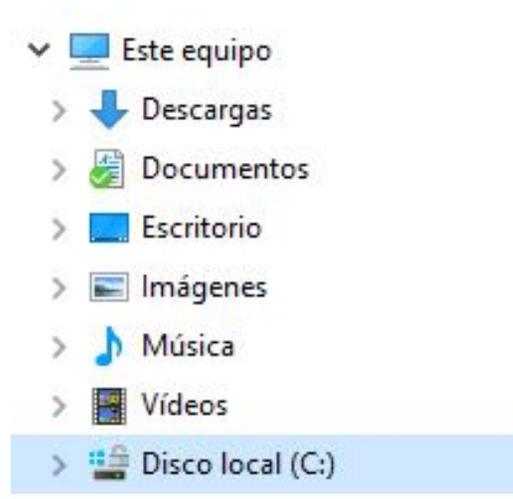


La ubicación **no** es una carpeta o archivo que ya existe – VeraCrypt creará un volumen (carpeta virtual) nuevo en el lugar que escoges. En la captura de pantalla, *C:/Users* es la ubicación y *Enanitos_Verdes* es el nombre que escogí para el volumen, dentro del cual almacenaré mis archivos sencillos.

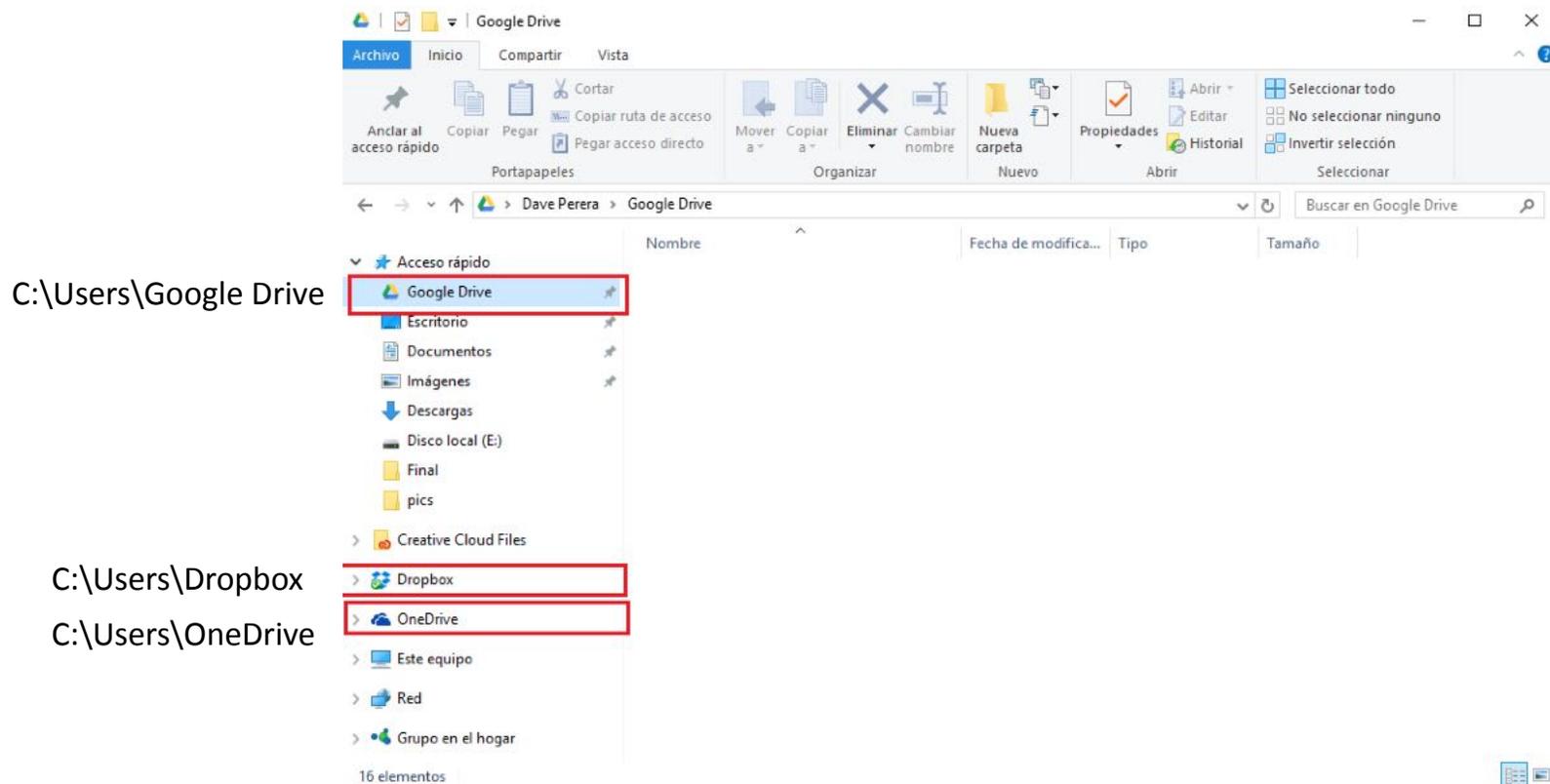
(“Enanitos_Verdes” primero porque mejor no escoger un nombre como “Archivos secretos” y segundo porque Lamento Boliviano: https://www.youtube.com/watch?v=khbDnLqe_Wk)



- C: es la letra más común para discos duros en el sistema operativo Windows.
- Si tienes dudas sobre la letra asignada al disco duro tuyo, comprabalo por Explorador de archivos, donde verás la letra debajo de “Este equipo.”



Si tienes cuentas de almacenamiento de la nube y son integrados con tu computadora, puedes también escoger una ubicación en la nube



C:\Users\Google Drive

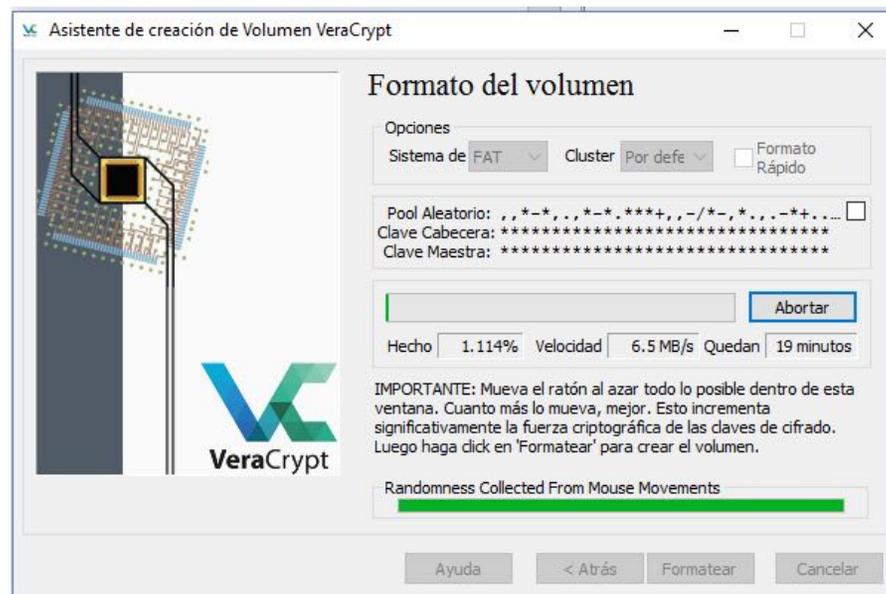
C:\Users\Dropbox

C:\Users\OneDrive

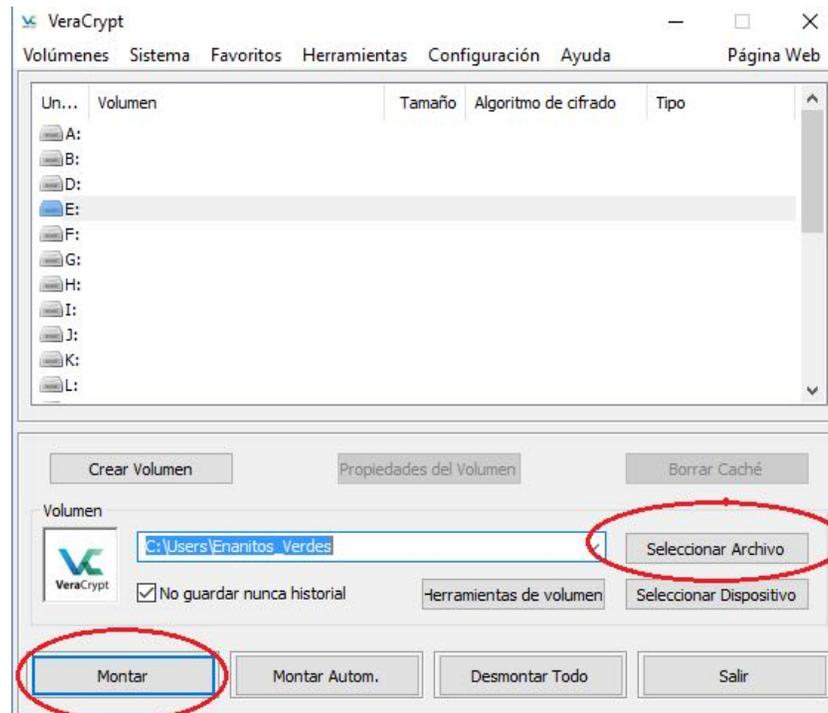
Tienes que escoger el tamaño del volumen. Obviamente depende del tamaño de disco duro y cuanto espacio vacío tienes disponible.



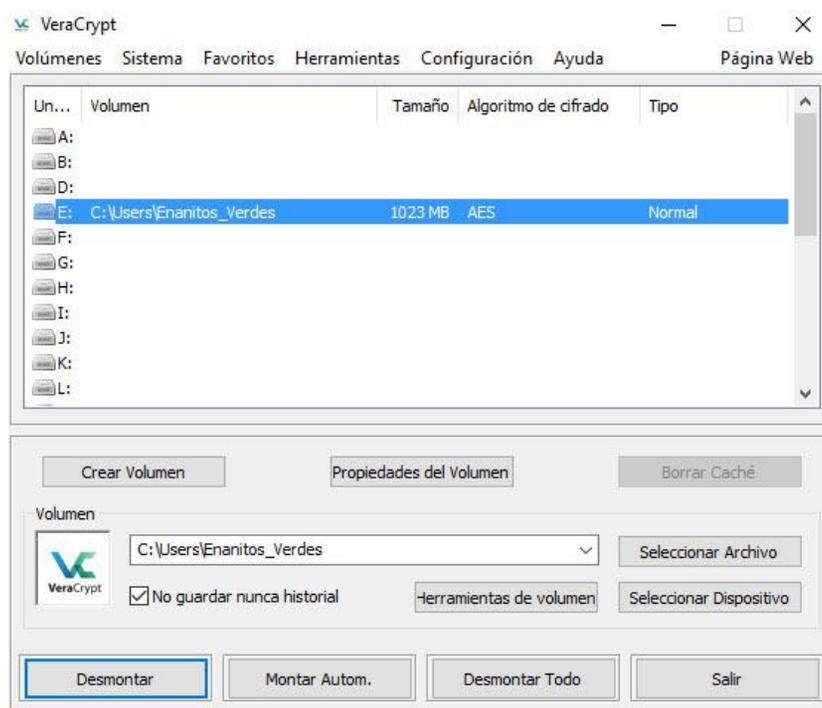




Para abrir el volumen, hay que montarlo. En este caso , haz clic en Seleccionar Archivo, y haz clic sobre el volumen en la ventalla que aparece. Después, haz clic in Montar.



Clickea dos veces el volumen y podrás añadir archivos. Cuando termines, no olvides desmontar el volumen.



Apéndice F – Otras aplicaciones para encriptar una entera maquina Windows

VeraCrypt

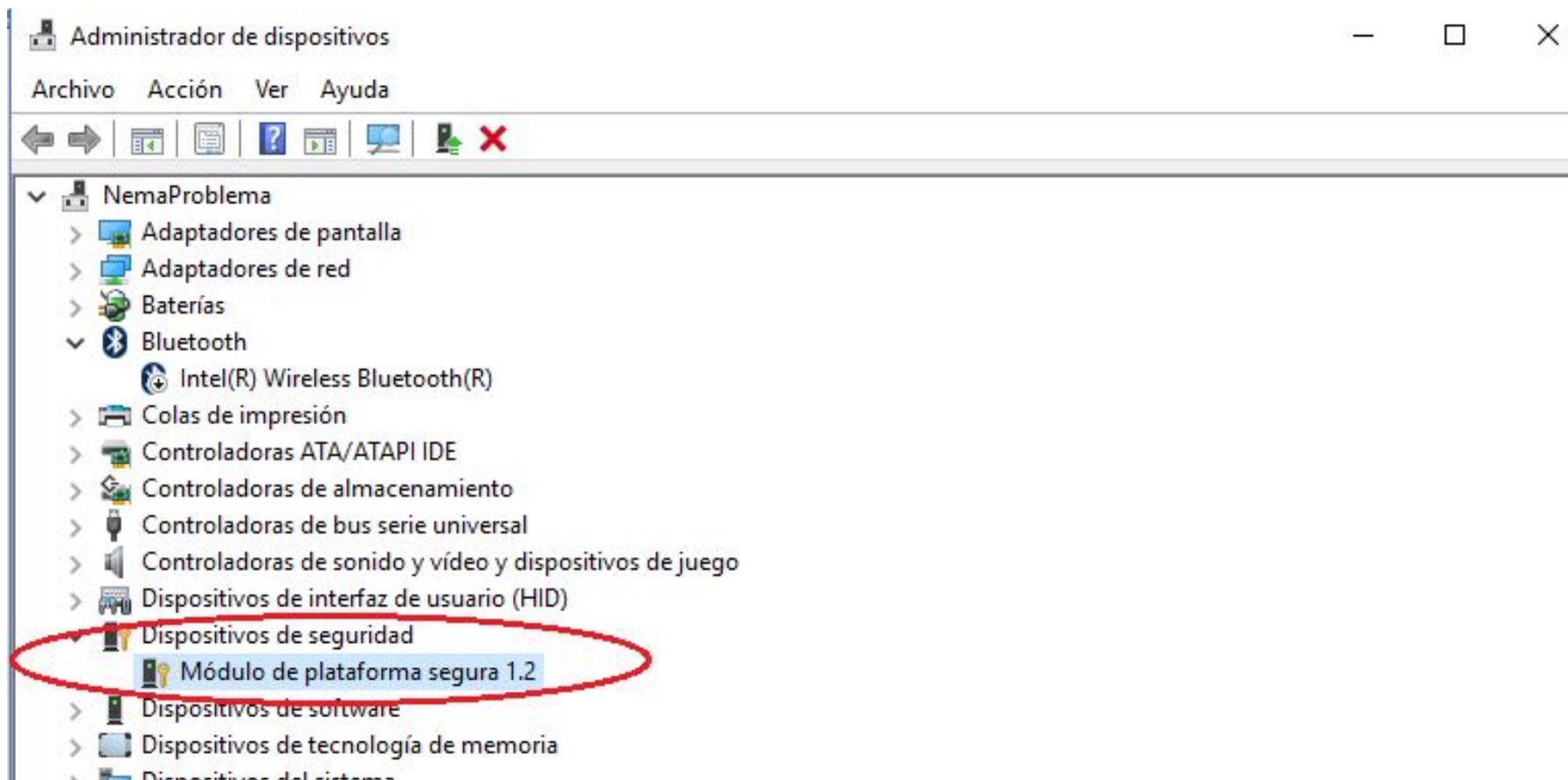
- VeraCrypt puede ofrecer complicaciones si deseas encriptar un entero disco duro con sistema operativo Windows.
- Para ustedes, otro problema más molesto que descalificador es una limitación con la contraseña por el previo al inicio de la computadora. Esta contraseña tiene que estar escrito en inglés (como se fuera el teclado un teclado con todas las claves en orden para inglés, no para español).
- VeraCrypt sigue siendo una opción buena para encriptar dispositivos USB or para crear volumens especiales

- **BestCrypt** es un programa propietario que tiene la recomendación de un criptólogo famoso llamado Bruce Schneier: <https://www.jetico.com/online-shop/shop/index/encrypt>
- **Symantec EndPoint Encryption** es otro programa propietario hecho por una de las firmas de ciberseguridad más grandes en el mundo, Symantec: <https://www.symantec.com/products/information-protection/encryption/endpoint-encryption>
- **DiskCryptor** es otra gratuita variación de TrueCrypt. https://diskcryptor.net/wiki/Main_Page

Apéndice G – BitLocker para encriptar un entero disco duro de sistema operativo Windows

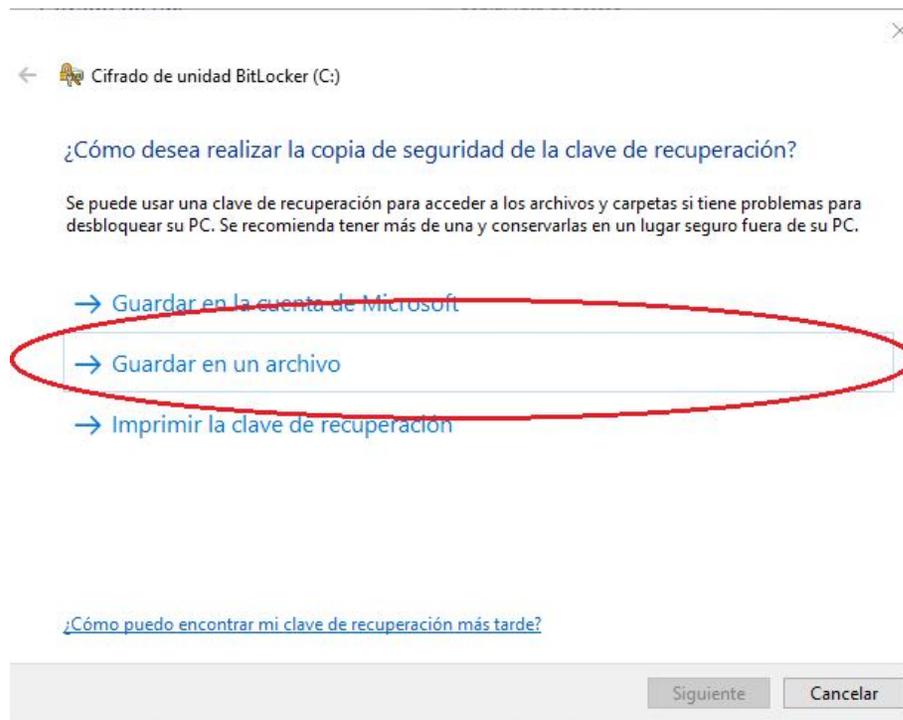
- La primera cosa que tienes que comprobar es si tu computadora tiene algo llamado el módulo de plataforma confiable, o un “chip TPM” por las siglas en inglés (Trusted Platform Module).
- Los TPMs son bastante comunes en computadoras hechas recientemente, pero no todas lo tiene.
- Para verificar si tienes uno:

Panel de control → Administrador de dispositivos → Verifica que hay “módulo de plataforma segura” debajo “Dispositivos de seguridad”

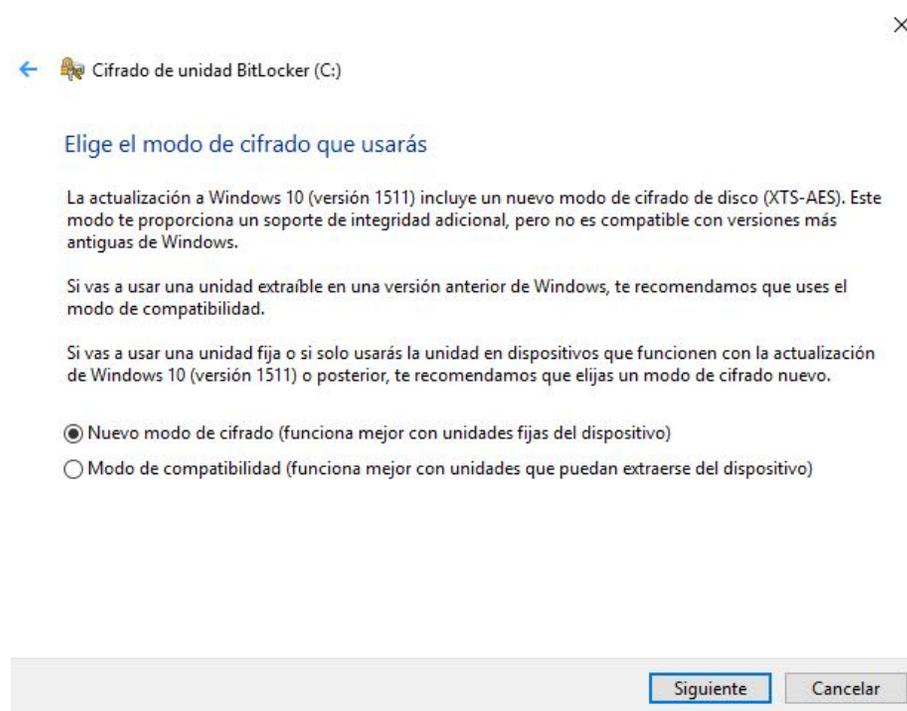


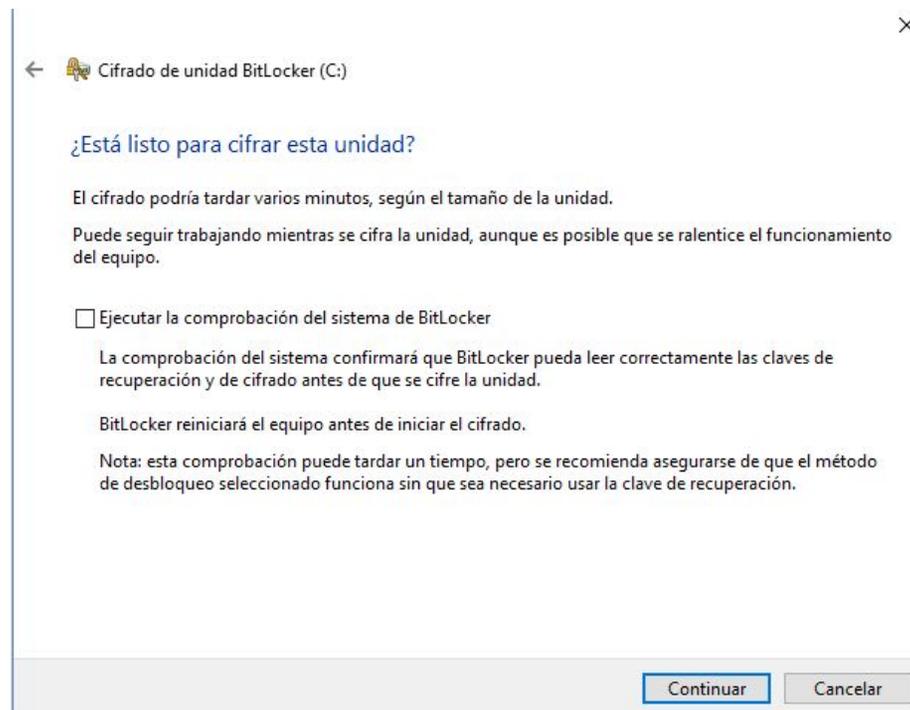
- Si sí, la tarea es bastante sencilla, si además tienes la versión correcta de Windows: Windows 8 Professional, Windows 8 Enterprise, Windows 10 Pro o Windows 10 Enterprise.
- Si tienes Windows Home, puedes comprar una actualización a una versión Pro. Las instrucciones están aquí:
<https://support.microsoft.com/es-mx/help/12384/windows-10-upgrading-home-to-pro>
- Si no tienes módulo de plataforma segura, consulta Apéndice I
- El proceso de encriptación durará un par de horas
- Panel de control → Cifrado de unidad BitLocker → Activar BitLocker

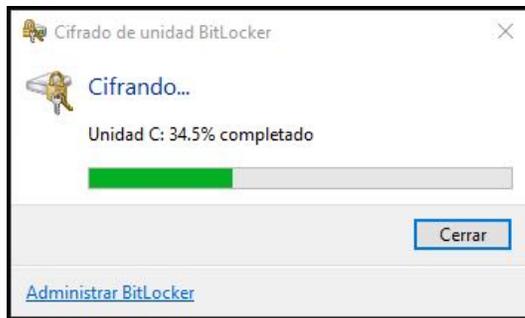
Recomiendo que no escoges la opción de guardar una copia de la clave de recuperación con una cuenta de Microsoft. Guardala en un dispositivo USB encriptado.



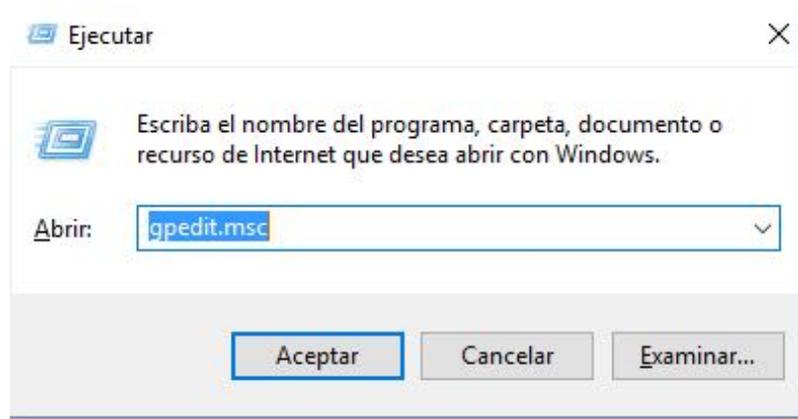
Si tu sistema operativo es Windows 10, escoge “Nuevo modo de cifrado.” (Bitlocker hace esta pregunta porque es posible también encriptar dispositivos USB utilizando el programa.)







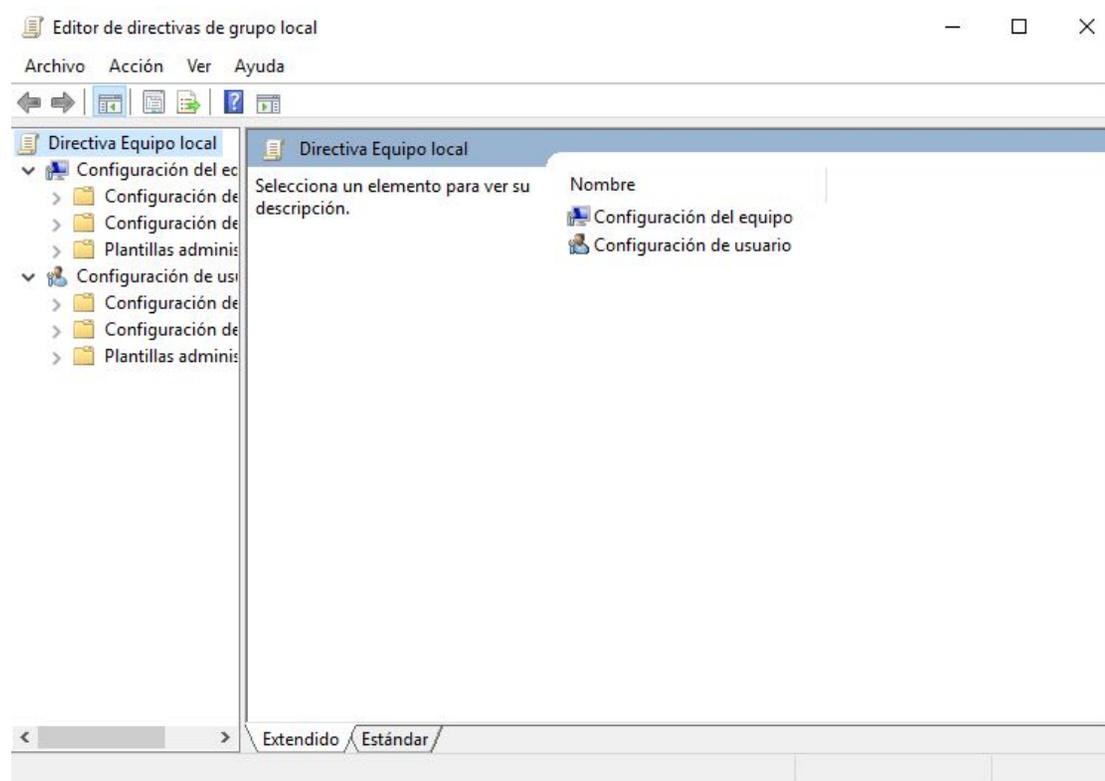
- Cuando esté completa la encriptación, Windows te avisará.
- Pero el proceso de fortalecer el equipo no ha terminado.
- El disco duro está encriptado, pero para asegurarse que tienes la mejor seguridad, añade un PIN.
- Un PIN previene que la clave de desencriptación sea cargada automáticamente en la memoria cuando enciendas la computadora.
- Es decir, un PIN previene que alguien pueda iniciar sesión de la computadora sin conocimiento de tu PIN
- Para empezar presiona  + R
- En la ventana, escribe: gpedit.msc



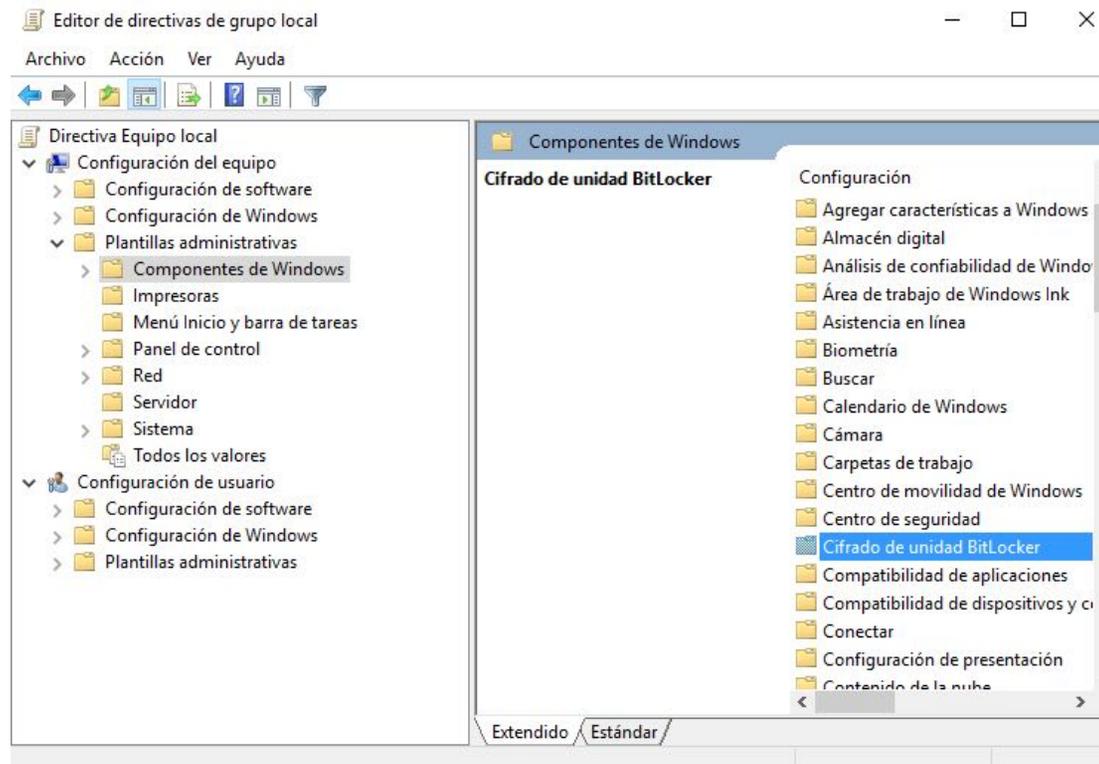
“gpedit” significa “editar política de grupo” (**g**roup **p**olicy **e**dit).

Dice “grupo” pero en este caso, el grupo consiste soloamente de tu computadora.

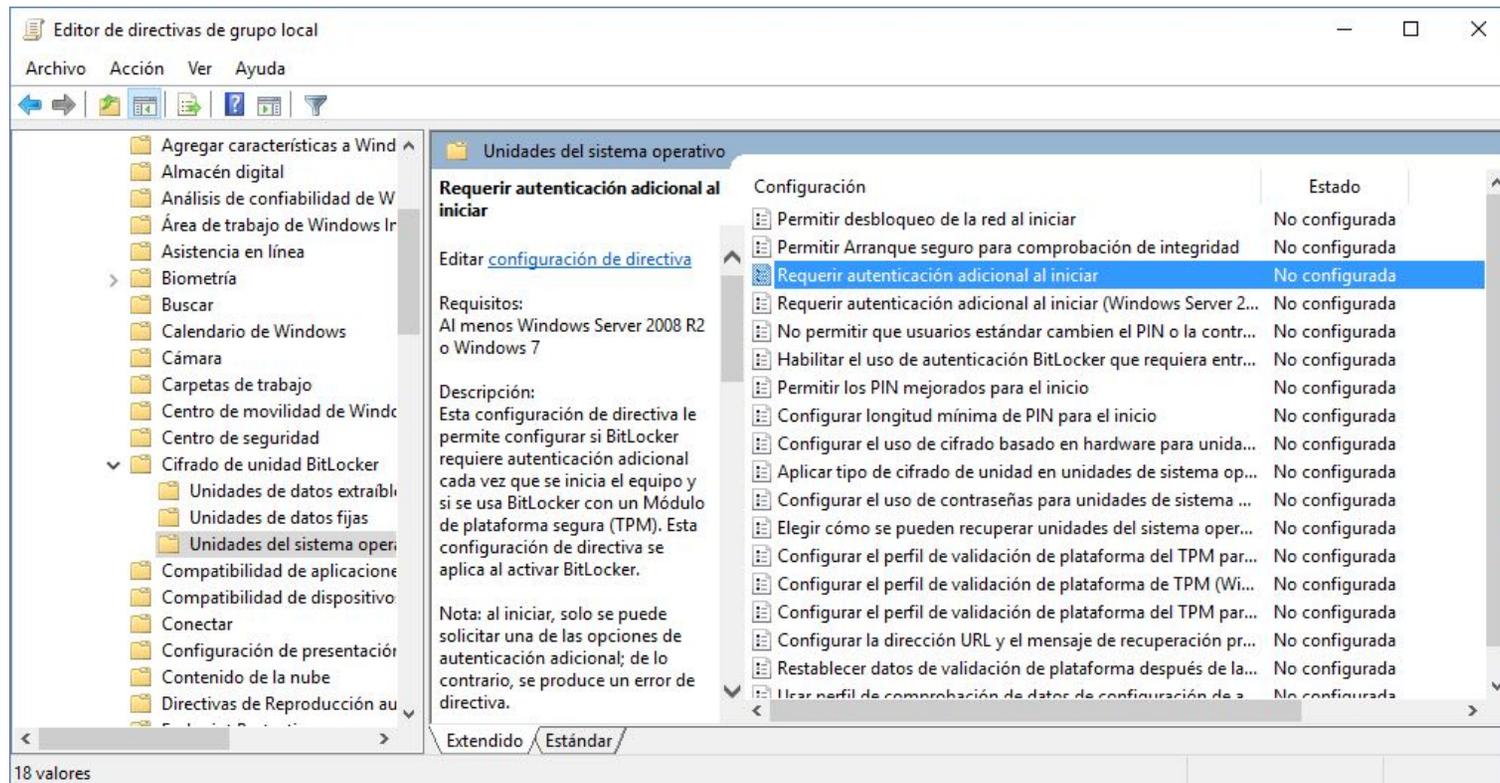
Este es la ventana que abre.



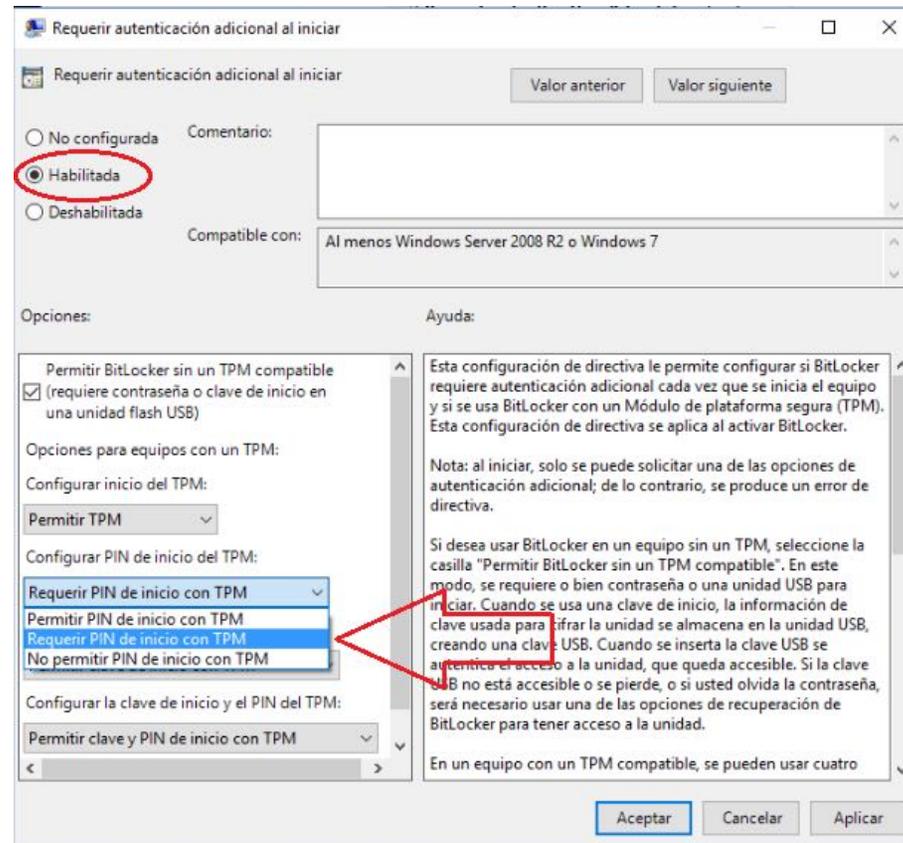
Abre Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker



Unidades del sistema operativo → Requerir autenticación adicional al iniciar.
Haz clic dos veces.

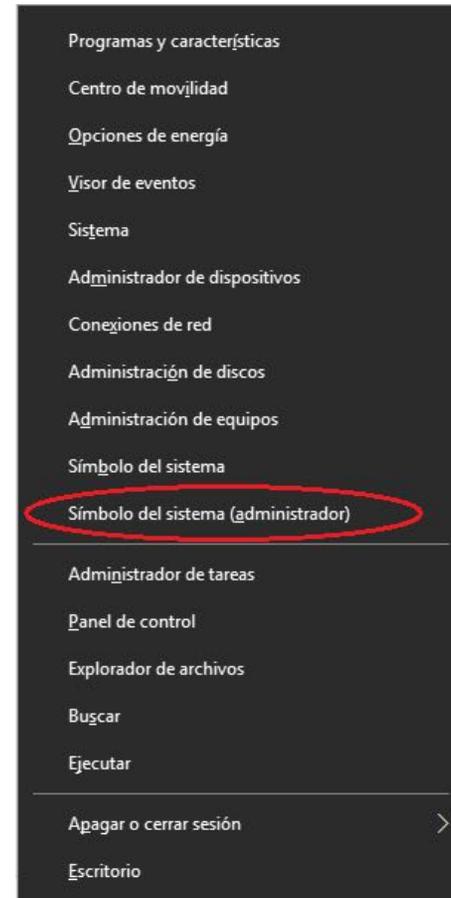


Selecciona “Habilitada” y escoge “Requerir PIN de inicio con TPM.” Cliquea “Aceptar.”



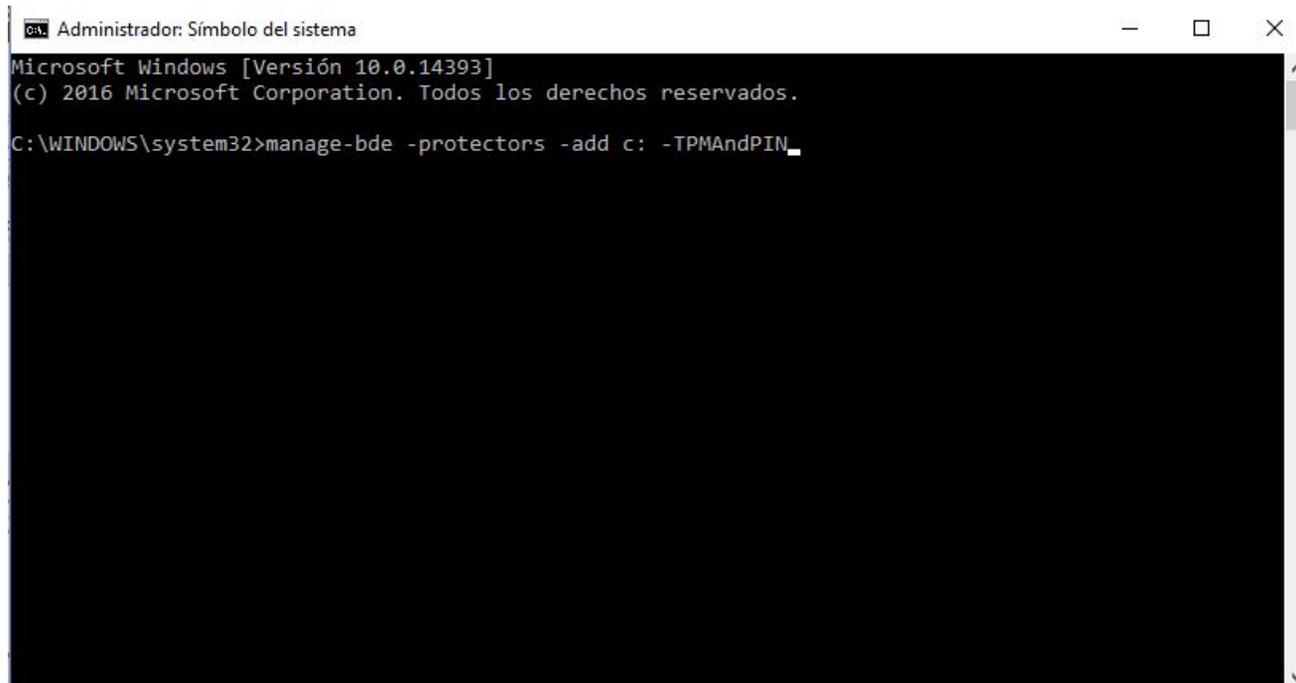
Entonces, hay que escoger el PIN.

- Presiona  + X
- Selecciona Símbolo del sistema (administrador)



En la ventana, escribe:

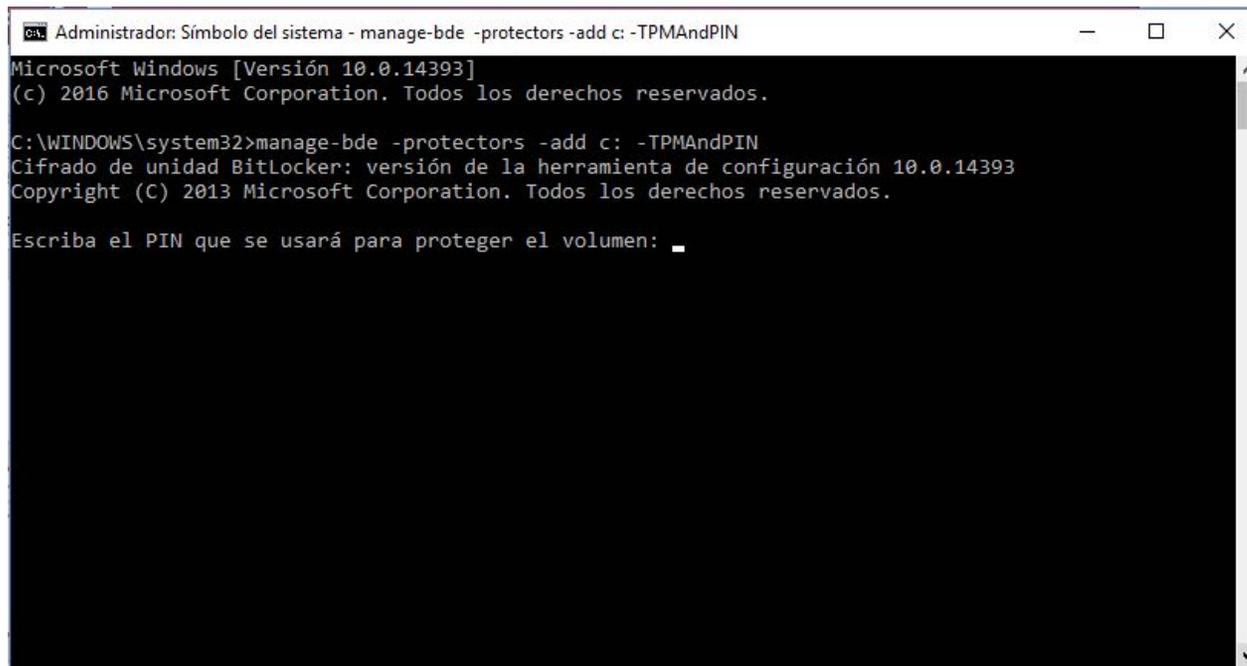
`manage-bde -protectors -add c: -TPMAndPIN`



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>manage-bde -protectors -add c: -TPMAndPIN_
```

Escribe el PIN



```
Administrador: Símbolo del sistema - manage-bde -protectors -add c: -TPMAndPIN
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>manage-bde -protectors -add c: -TPMAndPIN
Cifrado de unidad BitLocker: versión de la herramienta de configuración 10.0.14393
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

Escriba el PIN que se usará para proteger el volumen: _
```

```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>manage-bde -protectors -add c: -TPMAndPIN
Cifrado de unidad BitLocker: versión de la herramienta de configuración 10.0.14393
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

Escriba el PIN que se usará para proteger el volumen:
Escriba otra vez el PIN para confirmarlo:
Protectores clave agregados:

    TPM y PIN:
    Id.: {EB517CAE-3503-409D-9917-06F53AE2AA75}
    Perfil de validación de PCR:
        0, 2, 4, 11

Se eliminó el protector de clave con el identificador "{D2216231-B033-434B-AB8E-C6D425C49877}".

C:\WINDOWS\system32>
```

Nota que Windows ha eliminado un protector de clave. En el proceso de añadir el PIN, el sistema operativo ha sustituido un nuevo protector de clave por el viejo que eliminó. El siguiente paso será comprobar que la encriptación funciona como debe y en caso afirmativo, no hay nada para preocuparse por el hecho de un protector de clave eliminado.

Verifica que el disco duro está encriptado con este mando:
manage-bde -status



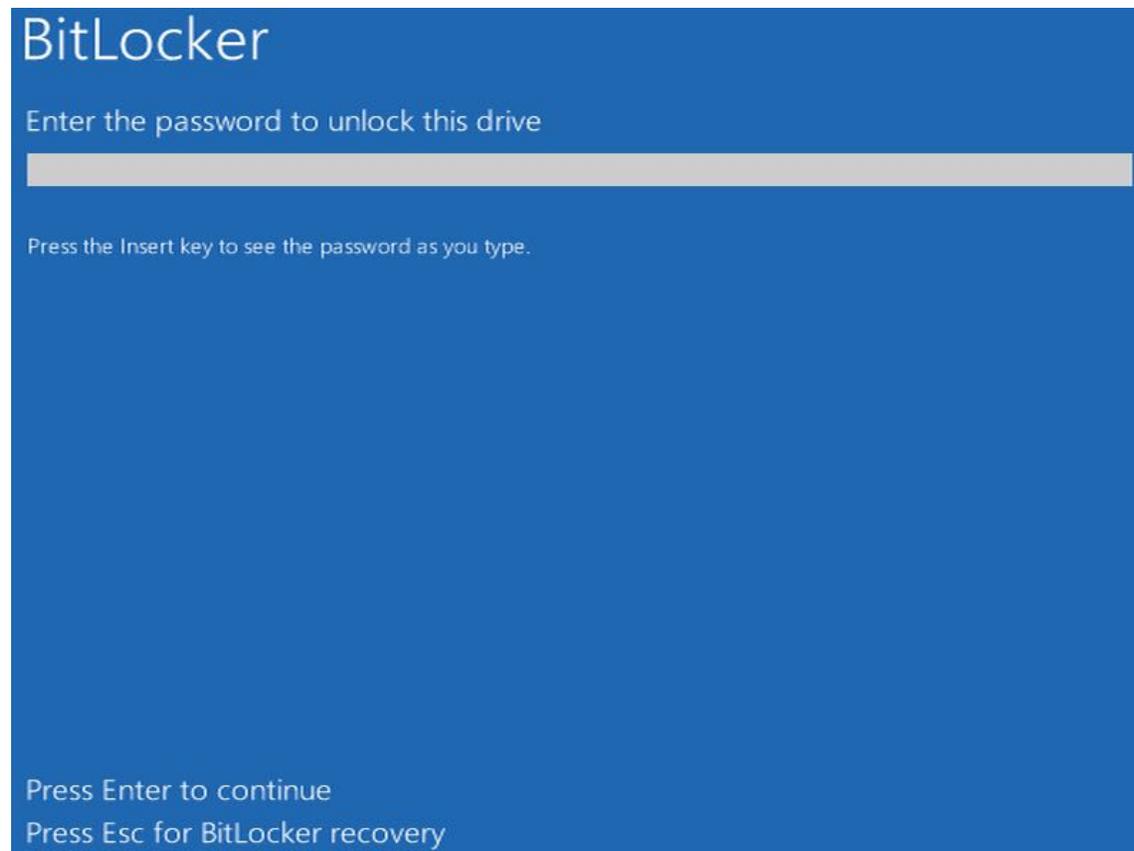
```
Administrador: Símbolo del sistema
C:\WINDOWS\system32>manage-bde -status
Cifrado de unidad BitLocker: versión de la herramienta de configuración 10.0.14393
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

Volúmenes del disco que se pueden proteger con el Cifrado de unidad
BitLocker:
Volumen C: [ ]
[Volumen del sistema operativo]

Tamaño:                222.62 GB
Versión de BitLocker:   2.0
Estado de conversión:  Cifrado completo
Porcentaje cifrado:    100.0%
Método de cifrado:     XTS-AES 128
Estado de protección:  Protección activada
Estado de bloqueo:     Desbloqueado
Campo de identificación:Desconocido
Protectores de clave:
    Contraseña numérica
    TPM y PIN

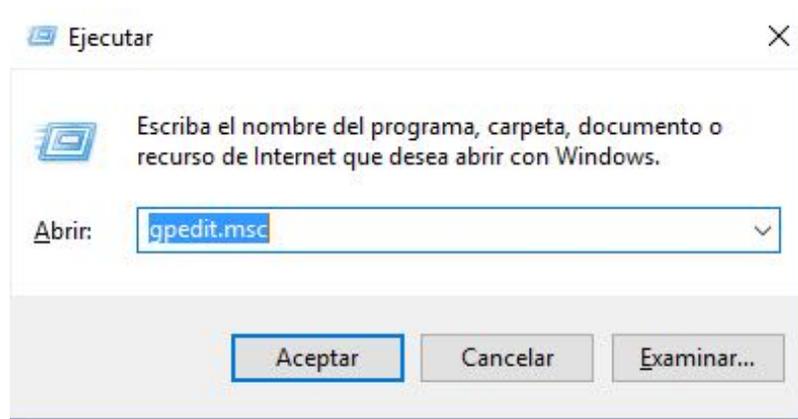
C:\WINDOWS\system32>
```

Desde ahora, cada vez que enciendes la computadora, verás esta pantalla:



Apéndice H – BitLocker sin módulo de plataforma confiable

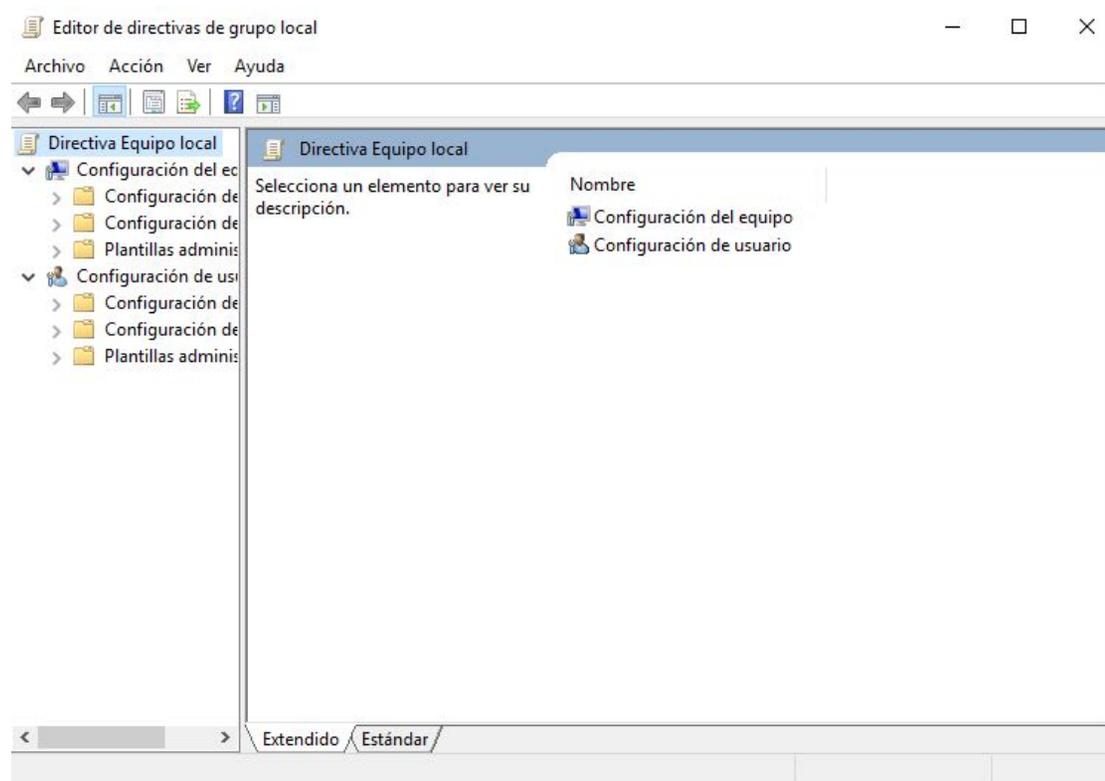
- Comprueba que tienes la versión correcta de Windows: Windows 8 Professional, Windows 8 Enterprise, Windows 10 Pro o Windows 10 Enterprise.
- Si no, puedes actualizar el sistema operativo a través de Microsoft Shop (hay un costo)
- Para empezar presiona  + R
- En la ventana, escribe: gpedit.msc



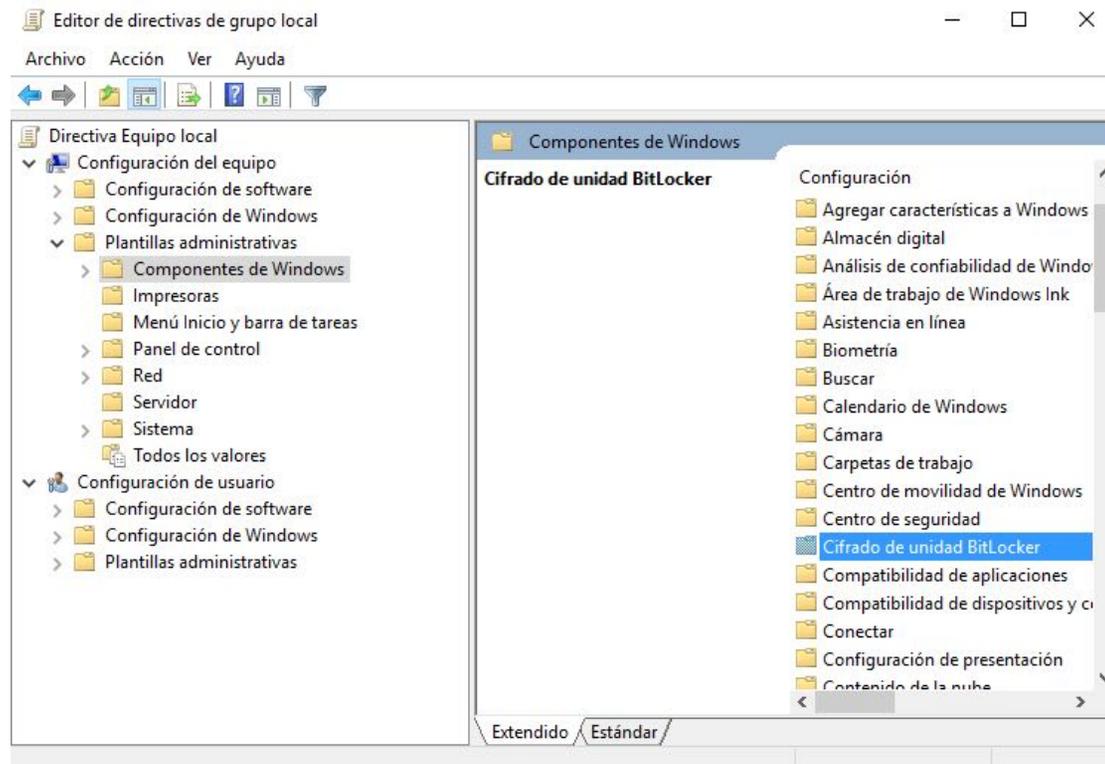
“gpedit” significa “editar política de grupo” (**g**roup **p**olicy **e**dit).

Dice “grupo” pero en este caso, el grupo consiste soloamente de tu computadora.

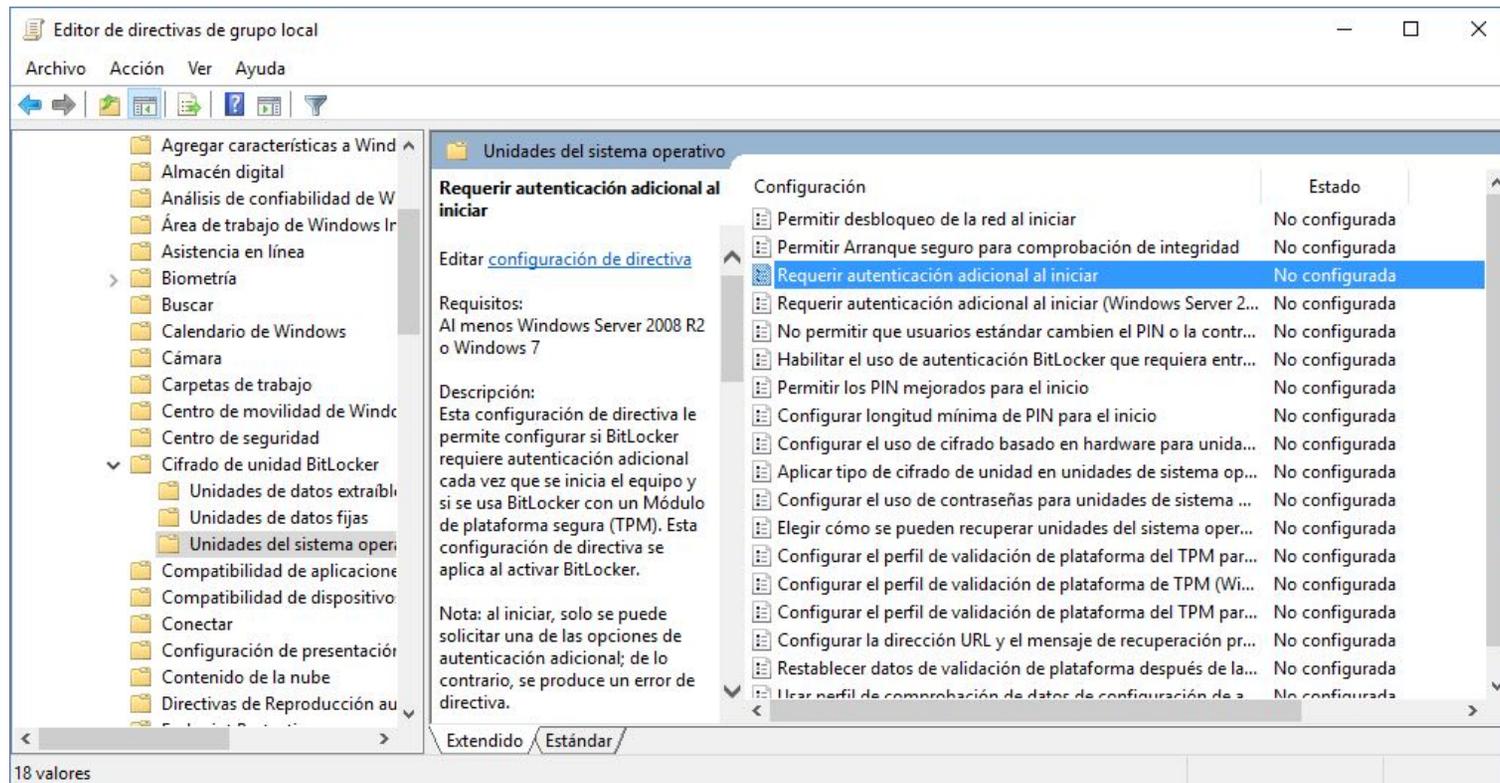
Este es la ventana que abre.



Abre Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker



Unidades del sistema operativo → Requerir autenticación adicional al iniciar.
Haz clic dos veces.



Escoge Habilitada y revisa la caja que dice “Permitir BitLocker sin un TPM compatible

Requerir autenticación adicional al iniciar

Requerir autenticación adicional al iniciar

Valor anterior Valor siguiente

No configurada Comentario:

Habilitada

Deshabilitada

Compatible con: Al menos Windows Server 2008 R2 o Windows 7

Opciones:

Permitir BitLocker sin un TPM compatible (requiere contraseña o clave de inicio en una unidad flash USB)

Opciones para equipos con un TPM:

Configurar inicio del TPM: Permitir TPM

Configurar PIN de inicio del TPM: Permitir PIN de inicio con TPM

Configurar clave de inicio del TPM: Permitir clave de inicio con TPM

Configurar la clave de inicio y el PIN del TPM: Permitir clave y PIN de inicio con TPM

Ayuda:

Esta configuración de directiva le permite configurar si BitLocker requiere autenticación adicional cada vez que se inicia el equipo y si se usa BitLocker con un Módulo de plataforma segura (TPM). Esta configuración de directiva se aplica al activar BitLocker.

Nota: al iniciar, solo se puede solicitar una de las opciones de autenticación adicional; de lo contrario, se produce un error de directiva.

Si desea usar BitLocker en un equipo sin un TPM, seleccione la casilla "Permitir BitLocker sin un TPM compatible". En este modo, se requiere o bien contraseña o una unidad USB para iniciar. Cuando se usa una clave de inicio, la información de clave usada para cifrar la unidad se almacena en la unidad USB, creando una clave USB. Cuando se inserta la clave USB se autentica el acceso a la unidad, que queda accesible. Si la clave USB no está accesible o se pierde, o si usted olvida la contraseña, será necesario usar una de las opciones de recuperación de BitLocker para tener acceso a la unidad.

En un equipo con un TPM compatible, se pueden usar cuatro

Aceptar Cancelar Aplicar

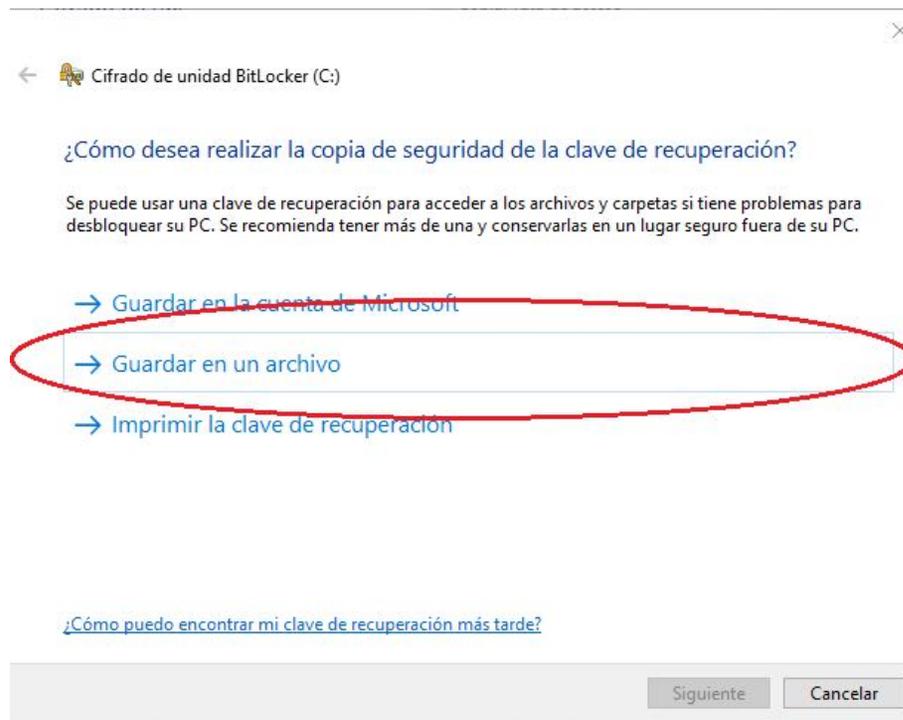
Dos opciones: Usa un dispositivo USB como un clave, o escoger una contraseña para desincryptar el disco duro cuando enciendes la computadora.

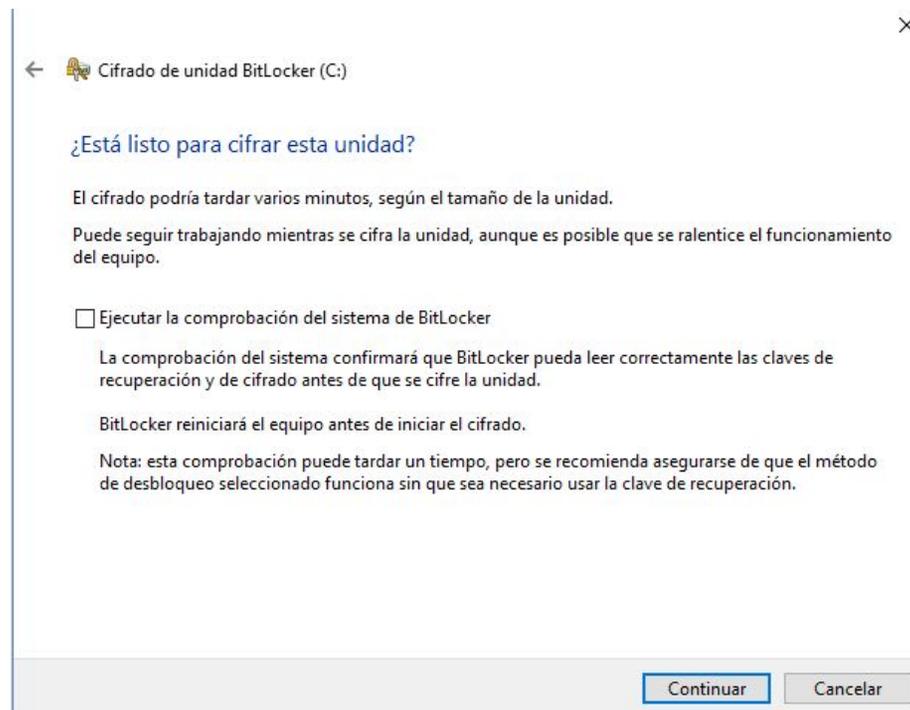
Si escoges el dispositivo USB, tendrás que tenerlo enchufado en el puerto USB cada vez que enciendes la computadora. ¡Ojo que no lo pierdes!



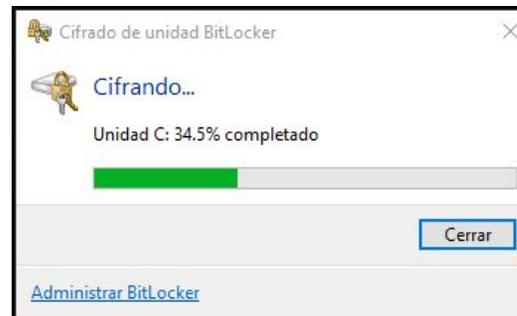
Para empezar la encriptación, ve por Panel de control → Cifrado de unidad BitLocker → Activar BitLocker

Recomiendo que no escoges la opción de guardar una copia de la clave de recuperación con una cuenta de Microsoft. Guárdala en un dispositivo USB encriptado.





- Cuando esté completa la encriptación, Windows te avisará.



Desde ahora, cada vez que enciendes la computadora, verás esta pantalla:

