Como Evitar el Espionaje de E.E.U.U,

y, otras Prácticas Soluciones Informáticas:

Proteger tu Pc, **Seguridad en Internet**,

AutoHacking, etc….

AbundioTeca

En la presente guía, vamos a ofreceros un conjunto de medidas que resuelven problemas de Seguridad comunes para todos los Internetistas: Navegación (Anonimato en la Web), Protección de Datos (Archivos), Hacking Malicioso, Protección del Pc, Comunicaciones en la Red 100 % Seguras, etc.

Todas las Herramientas e Información que ofrecemos a continuación son gratuitas, libres, y, legitimas, no obstante, su uso y aplicación es vuestra decisión.

Bloquear Pc (Intrusión Física): Una de las formas mas sencilla, efectiva, y, preferida por los intrusos para controlar vuestro ordenador es a través de un punto físico directo, es decir, acceder a vuestro dispositivo por un puerta que habéis dejado abierta, vamos, como si dejáseis las llaves de casa puestas.

Si aun no habéis creado una cuenta de usuario en WindOUs, id a Panel de Control > Cuentas de Usuario, y, modificar la de Usuario con una contraseña segura que incluya mayúsculas, minúsculas, números, y, caracteres.

¿Y para que sirve esta solución?, Si vuestra maquina esta continuamente encendida, y, conectada a la red permanentemente, en algún momento puede entrar cualquier intruso a vuestro pc. Para evitar su acceso mientras no estamos presentes, bloqueamos el pc directamente: en WindOUs, presionamos la teclas “Logotipo de WindOUs + L”, para Mac “ctrl. + Shift + Botón expulsar”, y, para Linux “Control + Alt + L”.

Nota: todo el software que propondremos a largo del manual, no esta enlazado directamente, solo esta comillado, razón, durante la lectura averiguaréis la motivación.

El anterior, es un método simple de **configuración de contraseña y teclado abreviado**, no obstante, también existen sistemas de acceso alternativos tales como; **reconocimiento facial**, huellas dactilares, tarjetas, etc.

Si tenéis una WebCam, podéis además añadir un método alternativo de bloqueo y acceso a través de reconocimiento facial; En WindOUs, podéis instalar "Blink o BananaScreen", que, son programas que graban y reconocen vuestro rostro en aras de fortalecer el acceso físico directo de intrusos, para Mac, "KeyLemon", y, para Linux, el paquete "PAM".

Pero, ¿Y **si han conseguido entrar** en vuestra maquina?, ¿Cómo averiguamos que ha pasado?, **Activar un Keylogger**, programa que graba todas las pulsaciones del teclado sin que el huésped se entere, puede ayudaros a saber que ha pasado y/o que esta haciendo el invasor. "Revealer Keylogger" puede serviros para realizar esta tarea

No obstante, si queréis proteger vuestra información mas relevante, realizad **copias de seguridad periódicas en un disco duro externo**.

Métodos Informáticos de Investigación Forense (Intrusión Remota): el ataque físico no es la única forma de entrar a vuestra maquina, también pueden acceder al equipo mientras esta encendido y conectado a una red de área local o Internet.

El **robo o consulta de información relevante**, destrucción de archivos, modificación de datos, etc., son las acciones mas comunes realizadas por los intrusos, ¿**Razones**?, la mayoría, con **fines monetarios**: adquisición de **contraseñas**, **sustracción** de información importante, vulneración de la **privacidad**, **copia** de valerosos archivos confidenciales, etc., No obstante, también acceden a nuestras maquinas para instalar Keyloggers con el fin de controlarlas para realizar **ataques masivos DDoS,** es decir, sobrecargar los recursos del sistema de la víctima para denegar sus servicios. Habréis oído hablar de este tipo de ataques dirigidos a páginas gubernamentales, y, sucedáneos institucionales.

Pero, todo este tipo de acciones dejan **huellas**, no obstante, existen herramientas para detectarlas siempre y cuando el intruso no sea un experto, siendo así, ¿Dónde las buscamos?, ¿Como actuamos?.

Si fuere experto, utilizaría herramientas para borrar sus huellas, algunas de ellas: borrado cache DNS con "DNSDATAView", borrado con "USBOblivion" de todas las memorias externas que hayáis conectado, borrar cache de flash y Java en la configuración de archivos temporales, limpiar el archivo de paginación "pagefile.sys" (interesados visitar este articulo http://support.microsoft.com/kb/314834), borrar archivos para siempre con "Hardwipe", si han sustraído información cambiaran fecha de modificación de archivos con "FileTouch", si han modificado algún archivo eliminaran o corregirán sus metadatos con "MetaStripper".

Todas estas técnicas, utilizadas habitualmente en el hacking malicioso, se conocen como anti-forenses, y, evitan la detección de rastros, no obstante, como las utilicéis si fuera el caso, es vuestra decisión.

Para cualquier otro usuario que no sepa como borrar sus huellas, sus actos dejan rastros en los registros donde se anotan los eventos más relevantes del sistema. En WindOUs, podéis consultar este **registro de eventos y aplicaciones** en Panel de Control > herramientas administrativas.
Servirá para detectar eventos registrados en momentos que estabais ausentes, y, por lo tanto descubrir que habéis sido atacados. En Mac, acudir a la carpeta "/private/var/log", además, el archivo kermel.log os indicara cuando se encendió la maquina y porque. En Linux, puedes utilizar el comando "lastlog" para saber si accedió algún intruso.

El sistema, software madre, no es el único que deja huellas, **otros programas** y archivos también pueden **contener miguitas de pan** tiradas por el intruso en: navegadores web, cache DNS, registros del router, caches de adobe flash y java, registro de trafico de red local, etc. Para borrarlas, el invasor puede utilizar "**CCcleaner"**, herramienta que recomendamos utilizar cuando terminéis cualquier sesión, consiguiendo así una efectiva virtual desintoxicación (cookies, caches, historiales, archivos temporales, scripts, etc.).

Tras realizar esta limpieza periódica, vuestra maquina será mas veloz y efectiva, no obstante, también deberéis quitar programas en desuso para aumentar la capacidad de computo de vuestra maquina.

Ahora, si queremos averiguar que **archivos** han podido ser **copiados**, "**OSForensics"** nos indica que archivos han sido abiertos y modificados recientemente. Para ello, debeis ir a la

carpeta “File Name Search” y buscar en la carpeta que sospeches ha sido objeto de copia. La lista, ordenada por el criterio *Access Time (desc)*, muestra los últimos archivos abiertos. Los archivos se pueden abrir con un visor interno que muestra los metadatos y los atributos de archivo originales sin modificar el archivo. Ahora bien, saber que ha modificado el intruso dependerá del conocimiento de tus propios datos. Para Mac y Linux podéis utilizar el comando “*find”*..

Si enchufaron USB u otras memorias en vuestro ordenador, “USBOblivion” también puede detectar estas huellas.

Si quieres **recuperar archivos borrados** en WindOUs, “OSforensics” también incluye esta opción de rescate; acudid a la carpeta “Deleted File Search”, y, “Save deleted file” en el archivo que queráis recuperar. Por otro lado, si habéis borrado archivos sin querer, “**Recuva”** es un programa que os ayudara a recuperarlos fácilmente. Para Mac, “FileSalvage”, para Linux, “Scalpel”.

Para **recuperar claves de registro**, podéis utilizar “**Yaru**”, muy útil además para ver si el intruso ha eliminado o modificado claves.

Las **invasiones más comunes**, se realizan a través de aplicaciones legítimas de **servidores de control remoto**, mas conocidas como **Keyloggers**. Con esta herramienta, el intruso dejara una puerta abierta para volver siempre que le apetezca a recopilar información confidencial, y, le sea enviada tal y como estime oportuno. Además, es posible que deje carpetas ocultas en el disco duro para ser utilizadas mas tarde en nuevas invasiones.

La captura de datos mas comunes se realiza a través de un **Keylogger** que **recoge las pulsaciones del teclado y las almacena en un archivo.** Los más sofisticados, incluso toman capturas de pantalla y atrapan contraseñas. Imaginad, con esta captura de datos podrá acceder a toda nuestra información relevante. El más conocido y efectivo para WindOUs es "***Revealer Keylogger***"

Pero, ¿Cómo detectamos estas aplicaciones?, un escaneo de cualquier programa **antivirus** podría detectarlo, pero, **no recomendamos instalar este tipo de software**, no por su ineficiencia, sino **por el consumo de recursos de nuestra computadora que ralentiza su funcionamiento**. Además, el *mayor virus de la maquina siempre es el usuario*, ya que siempre instalamos aplicaciones innecesarias e incompatibles con el rendimiento de nuestro ordenador.

Por lo tanto, **bastara con un antivirus LiveCD**, es decir, **discos de rescate que te ayudan a analizar y limpiar WindOUs sin iniciar sesión,** evitando así que se activen los virus para bloquear el sistema operativo cuando este se enciende, es decir, funcionan arrancando desde el cd.

Existen varias opciones, pero una de las más potentes, que, además incluye el navegador Firefox y recuperador de datos File Recovery, es "***BitDefender Rescue CD***". Para usar BitDefender Rescue CD, deberás grabar la imagen ISO en un disco CD y arrancar el ordenador desde él. En Linux, podéis utilizar "*rkhunter*".

Buscar entre los **procesos activos de memoria**, también puede serviros si queréis encontrar algo nuevo o extraño ejecutándose en vuestro sistema operativo. Para WindOUs, tenéis que abrir el administrador de tareas (ctrl.+alt+supr) y en la pestaña de procesos ver cuales no os resultan familiares.

Páginas como tasklist o Processlibrary elaboran listas con los procesos sospechosos más comunes, y, si encontráis alguno en vuestro administrador de tareas, eliminadlo. En Linux y Mac abrid la consola y escribid el comando ps para hallar todos los procesos activos.

Para descubrir las carpetas y/o archivos ocultos, "OSForensics". En la opción "File Name Search", en la pestaña resets de la interfaz, seleccionar la opción "Hidden atribute set". Para Linux y Mac, abrid la consola y escribid el comando *find /ruta/ -iname ".*" -maxdepth 1 -type f,*

Una de las **soluciones mas potentes para prevenir el acceso** de intrusos es **cifrar todo tu disco duro**, es decir, encriptarlo, transformar los datos en un lenguaje incomprensible a no ser que se utilice una clave. Si optáis por esta opción, recomendamos el programa "***TrueCrypt***", no obstante, no olvidar nunca la clave maestra que generéis al encriptar toda vuestra información o perderéis el acceso a todos vuestros datos.

No obstante, si sois vosotros mismos los que queréis **borrar un archivo para siempre**, podréis utilizar las siguientes aplicaciones: "***Eraser***" para WindOUs, "*Permanent eraser*" para Mac, y, "*Wipe*" para Linux. Recordad, no basta con eliminar el archivo si queréis deshacerlos de el ya que esta opción solo libera el espacio del disco que ocupaba, tenéis que utilizad las anteriores herramientas.

Como Acceder a un Ordenador, Explorar su Contenido, y, Extraer toda la Información Relevante (**AutoHacking**): las herramientas que proponemos a continuación, sirven para buscar todo tipo de información en vuestra maquina, su ilegitima aplicación, es vuestra decisión.

El AutoHacking, tiene como objetivo principalmente recuperar información propia, o, de otros usuarios que nos autoricen. A continuación, enumeramos algunas de estas utilidades:

. Recuperar archivos: “DiskDigger”, “Recuva”.

. Rescatar correos borrados de Outlook Express: “Format Recovery”.

. Recuperar contraseñas almacenadas en el navegador: “BrowserPasswordDecryptor”

. Rescatar contraseñas de Messenger, yahoo, etc: “MessenPass”.

. Recuperar las contraseñas de cuentas de correo locales (Outlook, thunderbird): “MailPassView”.

. Obtener contraseñas de redes wi-fi: “WirelessKeyDump”.

. Para rastrear Caches (residuos de navegación) e Historiales: “Chat Sniper” (recopila historiales, imágenes y contactos de Messenger), “MozillaCacheView” (exploran las caches cuando navegas), “MyLastSearch” (almacena las ultimas búsquedas realizadas), “flashCookieView” (analiza las cookie flash), “SkypeLogView” (compila todas las llamadas hechas por Skype), etc.

. Para buscar documentos y/o texto; “DocFetcher”.

. Para buscar en los adjuntos de Outlook: “OutlookAttachView”.

. Para buscar en los adjuntos de Thunderbird: “MozBackup”.

. Para Recuperar Imágenes Borradas: “AdroitPhotoRecovery”

. Para explorar el disco duro en aras de ver su reparto: “SpaceSniffer”.

. Para comprobar archivos en uso, o, programas abiertos: “OpenedFilesView”.

No obstante, **la mas completa** de todas las herramientas es, “***OSForensics***”, un suite muy potente que incluye todo tipo de utilidades; buscador de texto, analizador de actividad reciente, búsqueda de archivos borrados, visor de memoria y disco, etc.

Insistimos, todas estas Herramientas son legítimas, aptas para AutoHackearnos en aras de recuperar, almacenar, y/o utilizar información propia tal y como estimemos oportuno, no obstante, otro uso o aplicación, es vuestra decisión.

Seria apropiado descargar todas estas herramientas directamente de sus paginas oficiales, actualizando periódicamente a nuevas versiones que mejoren el rendimiento de la maquina, ya que, si lo hacéis desde plataformas que ofrecen estos programas, podéis ser infectados por software de publicidad intrusivo (adware), y/o, navegadores cookie captores, que, ambos casos ralentizan e incluso controlan vuestra maquina.

Las **cookies** son como las **bolsas de la compra, sirven para revelar que tiendas visitáis**, y, este tipo de paginas autoinstalan en vuestro ordenador un propagandístico navegador, que, capta información de vuestros hábitos de búsqueda, para, venderlos a corporaciones interesadas.

No obstante, esta información también es captada por las paginas oficiales de descarga de software libre, pero, la contribución voluntaria que realizamos es distinta, ya que, los datos que aportamos les sirven para; mejorar su producto en aras de aumentar la experiencia de navegación del usuario, y, ofrecer por tanto nuevas herramientas dirigidas a satisfacer las necesidades reales del internauta, es decir, satisfacer la demanda real, no crear oferta artificial.

Sirva el navegador Firefox como ejemplo, donde, recomendamos instalar el complemento "Self-Destructing Cookies", para que, una vez obtengan nuestra información, se destruyan las cookies sin ser almacenadas en nuestra maquina.

Además, seria conveniente activar el **Firewall**, Cortafuegos, para **gestionar y filtrar la totalidad de tráfico entrante y saliente** que hay entre dos redes u ordenadores de una misma red.

Debemos establecer unas **reglas que debe cumplir el tráfico**, y, **si no las cumple, será bloqueado**. Por lo tanto, configurar correctamente esta herramienta es una tarea muy importante, ya que, nos protege de los intrusos, bloqueando además cualquier tipo de tráfico malicioso.

Algunas de las **reglas** que podemos implementar son: administrar el acceso de los usuarios a los servicios privados de la red, registrar todos los intentos de entrada y salida de una red (logs), filtrar direcciones para bloquear o aceptar el acceso a nuestro equipo de IPs a través del puerto 22, filtrar protocolos para rechazar o permitir trafico en función de su tipología (http, https, TCP, FTP, etc.), controlar el numero de conexiones que se estén produciendo desde un mismo punto para bloquearlas en caso de que superen un numero

determinado, controlar las aplicaciones que pueden acceder a Internet para restringir su uso a ciertos usuarios, detección de puertos que están en escucha para advertirnos de aplicaciones no amigables que quieren utilizar un puerto para esperar conexiones entrantes,……

Ahora bien, existe Firewall de dos tipos; Software, y, Hardware. El primero, es el más común, y, suele estar preinstalado en nuestro sistema operativo, que, podremos configurar teniendo en cuenta las reglas anteriores. No obstante, tal y como advertimos para los programas antivirus, esta opción consumirá bastantes recursos de vuestro ordenador, pero, es apropiado que este activado.

El segundo, dispositivos de **hardware firewall**, son una **excelente solución** para proteger cualquier red. Incluyen funcionalidades como; CFS, tecnologías SSL (capas de conexión segura), VPN (redes virtuales privadas), antivirus integrados, antispam, control de carga, etc. Si optáis por este componente físico, acudir a vuestro informático de cabecera.

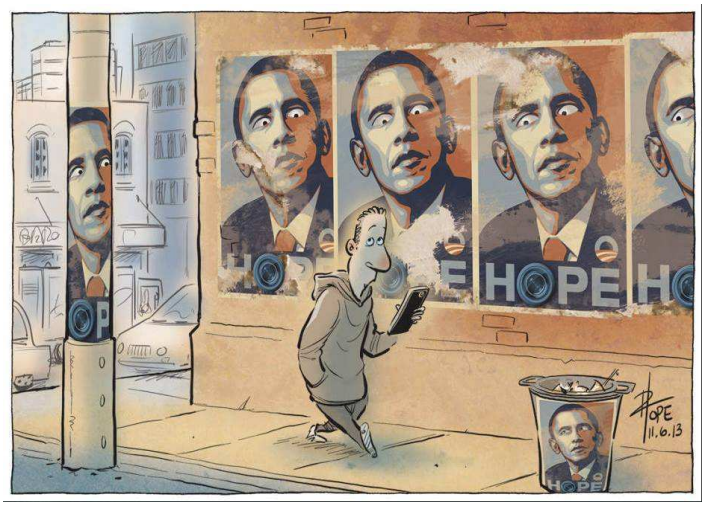
Las anteriores funciones; Bloquear Pc, AutoHacking, Gestión de Cookies, y, Proteccion Firewall, van dirigidas principalmente a impedir el acceso de intrusos, además de, recuperar información relevante, pero, si utilizamos frecuentemente la Red Mundial Global, Internet, estaremos expuestos a **otras amenazas** tales como la **vulneración constante de nuestra privacidad.**

Pero, ¿Por qué son tan importantes nuestros datos?, existen varios interesados en los mismos, pero, con diferentes fines;

. Gobiernos e Instituciones (**PermisoCracia**): perpetuar el dominio y control masivo sobre toda la sociedad, vigilando cada uno de sus pasos en aras de neutralizar cualquier movimiento y acción molesta que amenace la continuidad de la clase dominante creada por el fraudulento sistema monetario paralizante.

. Empresas (**CorporatoCracia**): Recabar Información a cerca de sus Consumibots (usuarios de bienes y servicios programadamente desinformados) para ofrecerles productos y servicios monetariamente interesados.

Efectivamente, nos espían.



Pero, ¿Cómo realizan esta tarea?, **a través de nuestra IP**, clave de identificación única necesaria para acceder a cualquier red.

Esta dirección permite a sus redes de vigilancia **establecer perfiles de todos los usuarios de Internet** a través del seguimiento por los sitios que visitan, y, **búsquedas** que realizan, localizándolos además geográficamente. Esta combinación de funciones es muy valiosa para todas las DES-Cracias.

Descartando usuarios estrella como Snowden o Assange (Wikileaks), que, liberalizaron información deshumanitaria, los objetivos de las anteriores DES-Cracias son principalmente monetarios, y, de control complementario.

Por desconocimiento de uso apropiado de las nuevas tecnologías, toda **la información que facilitamos voluntariamente** en la red **deja rastros que revelan nuestra identidad**, que, se **almacenan** en diferentes **bases de datos interesadas**.

Generalmente, **las utilizan con fines monetarios de menor grado**; **redes sociales, y, agencias de publicidad orientadas, actúan como plataformas de captación masiva**. No obstante, también sirve a organizaciones de planificación social como método de control efectivo.

Por lo tanto, anonimato, privacidad, y, seguridad en la red están programadamente ausentes, hasta que la siguiente herramienta se os presente: **Proyecto Tor**.

Tor, no hace referencia a ningún ser mitológico dueño del rayo, atiende a las siglas The Onion Router (El Router Cebolla).

Descuidad, no se trata de ningún dispositivo que provoca lagrimas cuando lo sacas de la caja, mas bien, hace referencia a su funcionamiento, es decir, es una **plataforma de muchas capas secretas**.

Para completar la teoría, copiamos y pegamos su valía: *En lugar de enviar la información de manera directa, por servidores tradicionales, Tor lo hace a través de diversos canales creados por voluntarios alrededor del mundo. La red de voluntarios de Tor brinda sus conexiones para que quienes las necesiten envíen información de manera segura, encriptada.*

Redirige aleatoriamente el tráfico del usuario a través de los varios nodos de voluntarios para ocultar su localización. Así, esconde las direcciones de Internet reales de los usuarios y cifra los contenidos de lo que están consultando. Su seguridad se asemeja a las capas de una cebolla.

Que si, también puede servir para **alojar contenidos cuestionables e ilegales** humanamente inaceptables, pero, también puede utilizarse para **fomentar los derechos humanos y/o libertades de expresión e información**, por lo tanto, **su uso y aplicación, dependerá de la humana programación**.

Las **decisiones del ser humano** son **producto del sistema socio-cultural monetariamente interesado**, donde, sus valores, costumbres, y, comportamientos, son fruto del adoctrinamiento temprano y programación social establecido.

Cualquier método de planificación social nunca ha sido dirigido hacia el cambio real que beneficie a toda la humanidad, únicamente busca preservar sus instituciones para perpetuarse en sus interesadas condiciones.

No obstante, las armas de control masivo que promueven: Propiedad Desfuncional, Escasez Artificial, y, Competencia desleal, serán superadas, y, sustituidas por Abundancia Sostenible, Cooperación Distribuida, y, Accesibilidad Universal.

Las **condiciones hostiles (trabajo, dinero, deuda) serán eliminadas** y surgirá una emergente sociabilidad fortalecida, ¿Cómo?, **aplicando humanitaria e inteligentemente Ciencia y Tecnología**.

La InHumanidad del sistema monetario será superada, desaparecerán todas sus ventajas competitivas representadas en las ganancias, y, **tan solo importara el bienestar del ser humano y medio ambiente**.

Estructuras permanentes, que, esclavizan a la humanidad a su mas lucrativo antojo, **caerán en desuso dejando paso a la nueva era de Cibernetica Social**, es decir, el matrimonio entre maquinas y ordenadores liberará a toda la sociedad a través de una **administración de Asuntos Humanos globalmente despolitizada, y, tecnológicamente avanzada.**

Se examinaran constantemente **nuevos paradigmas** con avanzados métodos actualizados, que, superaran el actual rezago neural tendente a resistir nuevos patrones a favor de los viejos ineficientes.

Por lo tanto, **dejaran de usarse cualquierismos que carecen de métodos globalmente efectivos**, para, aplicarse al sistema social común **escalas de funcionamiento científico altamente cualificadas**, basadas en los recursos y tecnología existente….

Descuidad, no estáis en una novela de Julio Verne, creemos conveniente explicar los **motivos que provocan el uso inapropiado de las nuevas tecnologías**, principalmente **causados por**; valores dominantes, que, rara vez surgen del pueblo, y, que son puntos de vistas programados para manipular a la gran mayoría sin parecer que han sido generados por instituciones monetariamente orientadas como gobiernos, milicia, bancos, iglesia, élites, etc.

Es decir, la contemporánea **patología social que sufrimos**, es el **resultado de las influencias que practican las anteriores organizaciones de planificación social ineficientes**, que, moldean y forman nuestro comportamiento socialmente inapropiado a través de valores, hábitos, creencias, y, costumbres, dirigidas servilmente hacia sus intereses creados.

La **pandemia sociopata monetariamente establecida**, que, produce un **trastorno del sistema valores**, tiene su origen en la fundación del inválido sistema monetario, que, genera condiciones hostiles tales como; deuda, dinero, competencia, propiedad, y, escasez.

Aplicando humanitariamente ciencia y tecnología, serian eliminadas, transformándose al mismo tiempo las emociones y relaciones humanas en una sociedad realmente fortalecida que superara el actual sistema de valores vitalmente distorsionado.

Expuesto lo anterior, esperamos que comprendáis el origen del comportamiento delictivo socialmente inefectivo, donde, la **conducta criminal**, humanamente desleal, es el **resultado de practicar cualquier escasez artificial**.

Recordad, **en un fraudulento sistema monetario, todos somos criminales**, ya que; **ningún recurso en su origen fue propiedad de nadie**, se nos obliga innecesariamente a **competir entre nosotros en condiciones de escasez virtual**, generando así violencia estructural como la pobreza y desigualdad humanamente desleal, y/o, también **nos beneficiamos de comportamientos delictivos que otros practican**. Pero, también esperamos que hayáis entendido como podemos provocar el cambio…….

Hasta la fecha, seguiremos **defendiéndonos con algunas de las herramientas aquí propuestas**. Bien, dejando al margen comportamientos humanamente aberrantes, y, ahora que sabéis que **no somos bienvenidos en organizaciones de planificación social p€oliticamente orientadas**, vamos a seguir explicándoos **como podemos incomodarles descubriendo sus intereses creados**, acelerando así el cambio esperado, el proyecto Tor, será nuestro aliado.

Esta herramienta permitirá vuestro anonimato en la red, ocultando vuestra dirección IP, garantizando que, vuestras comunicaciones web sean 100 % seguras.

Su instalación es muy sencilla, descargad el software desde su web oficial, y, ejecutarlo en vuestra maquina. Aparecerá en vuestro escritorio una carpeta denominada "Tor Browser", donde, encontrareis el icono "Start Tor Browser", pinchad sobre él, y, ya podéis navegar tranquilos en la intimidad de vuestras acciones.

No obstante, resultan curiosos algunos de sus patrocinadores como el laboratorio de investigación naval de EEUU, que, utiliza esta herramienta para proteger sus comunicaciones.

Hemos de advertir que, si descargáis esta aplicación, seréis susceptibles de investigación, no obstante, no debe ser preocupante si no tenéis un comportamiento aberrante, eso si, tened cuidado si decidís publicar información que moleste e incomode a la clase dominante.

Todas las DES-Cracias siguen el mismo patrón de conducta delictivo, ya que, solo intentan **preservar su sistema establecido**. Actualmente, nos encontramos en la primera fase de la secuencia, donde, **cuando nuevos movimientos dirigidos a provocar el cambio emergen**, suelen practicar habitualmente la **censura**, en este caso; alteran resultados de buscadores Web para frenar información relevante, cierran paginas que amenacen las ventajas de la corporatocracia monetariamente dominante, ridiculizan e ignoraran cualquier pensamiento critico hacia sus errores sistémicos, persiguen movimientos que intentan despertar consciencias, etc.,

No obstante, el cambio representado por toda la humanidad hacia una **Cibernética Social** seguirá su curso, e **Internet**, arma de divulgación masiva, que, ofrece información no sesgada sin filtrados puntos de vista, **liberará a toda la especie humana de la esclavitud monetaria**.

Estamos viendo como falla continuamente el actual sistema de mercado monetario, que, sufre un colapso acumulativo provocado por sus reglas del juego inherentemente inválidas, donde, solo importan las ganancias cíclicas, que, no tienen en cuenta los recursos finitos del planeta, ni, el bienestar general del ser humano. Hacia ese cambio nos dirigimos, estando muy próxima la segunda fase de la secuencia, el fallo inevitable del fraudulento sistema monetario.

Hasta entonces, Activistas, Militares, Periodistas, Bloggers, Corporativistas, Médicos, Elitistas, Espías, Hacktivistas, Banqueros, Credencialistas, Abogados, Matemáticos, Físicos, Policía, Químicos, Ingenieros, Escolarizadores, Economistas, Investigadores, Políticos, Propagandistas, Programadores, Internetistas, Desarrolladores, Sistemistas, etc., todos, están en la misma lista, tan solo les diferencia su orientado punto de vista.

En esta primera parte de la secuencia, **algunos** integrantes de la anterior lista **revelan soluciones alternativas al ineficiente método de planificación social existente**, p€olitica y economi$a vigente. **Otros**, la causalmente programada elite credencialista, **intentaran preservar las actuales ventajas que tan solo benefician a unos pocos**.

La p€olítica que practica cualquier demoGracia, es el escudo que les protege de la población desinformada, que, aun cree que la solución sigue siendo p€olítica, y, esto es así porque la gran mayoría desconocen como funciona el sistema monetario. La economí$a virtual de mercado monetario, tal y como la conocemos hasta ahora, es solo un libro de hechizos complejos de los magos de su corte, que, disfrazan el mecanismo del juego fraudulento.

Ni una ni otra son la solución tal y como las conocemos hasta la fecha, a las pruebas de desigualdad, pobreza, violencia estructural, y, corrupción sistémica, hay que remitirse.

Imaginad que vuestro cuerpo se basase en un sistema político-económico, ¿tendrían vuestras heridas el suficiente dinero para comprar las plaquetas que necesitan?, ¿o el partido socialista popular de la sangre unida decidiría sobre la cantidad que necesitáis?....Esperamos que nadie haya contestado.

La moralidad y ética que practican estos sistemas no son funcionales porque operan dentro de un sistema inválido, si, aplicásemos humanitariamente ciencia y tecnología, entonces los valores que defienden podrían ser apropiados. Espiritualidad, Ética, y, Moral, adaptados a una dirección Funcional, son la ciencia y tecnología en acción.

Por lo tanto, en esta **primera fase** de la secuencia, toda la humanidad descubrirá que un **nuevo modelo que nos beneficie a todos es posible**. No obstante, hasta que se produzca el cambio, seria apropiado plantear una **transición** de, la actual Desconomia Virtual de Mercado Monetario, a, una **Economia Real Productiva Socialmente Participativa**, es decir, mantener durante la transición un Humanitario Sistema Monetario, pero, Libre de Dinero-Deuda parasitario.

Interesados en consultar como provocar la anterior transición, visitad la página www.wikibolsa.org, categoría "Programa de Soluciones".

Podéis difundir cualquier movimiento o cambio a través de la red Tor, pero, ¿Por qué es tan importante el anonimato para divulgar información relevante?, simple, porque **manifestarse enfrentándose directamente contra las guardianes no sirve de nada**, tan solo justifica su actuación desmedida hacia enemigos que en ocasiones ni siquiera existen.

Es recomendable que el **mensaje nunca vaya dirigido a quienes realmente no les importa que suceda un cambio que nos beneficie a todos**, bien porque desconocen otros métodos realmente efectivos, bien porque sufren de identidad estática credencialmente programada, o bien porque disfrutan de ventajas sistémicas que únicamente benefician al 1 % de la humanidad que representan.

Utilizad armas de expansión masiva como la red global mundial (**www**) para alcanzar al resto de la humanidad, aproximadamente el 99 %. **Cuando la gran mayoría sepa que un cambio que nos beneficie a todos es posible,** sencillamente, **dejaran de usar las instituciones que les esclavizan**, acelerando así por tanto el colapso y fallo definitivo del sistema monetario.

Tor es anonimato, no confidencialidad, así que evitad registraros en paginas donde tenéis que aportar vuestros datos, si fuere necesario, emplead pseudónimos, y, la dirección de Papa Noel en el polo norte.

Los detractores de esta red de capas secretas, alegan que esta plataforma sirve para alojar servicios ocultos, no obstante, recordad que la tecnología puede utilizarse con diferentes fines, como se emplee, será responsabilidad final del usuario. Anteriormente veíamos cual era la solucion para evitar comportamientos aberrantes.

Actualmente, casi el 50 % de estos servicios ocultos van dirigidos a contenidos para adultos, armas, falsificaciones, y, drogas, nada que no realicen “legalmente” todas las DES-Cracias.

Respecto a las armas, los goRRiernos las fabrican y comercializan en masa perpetuando el rentable negocio de la guerra, respecto a las drogas, cualquier des-sanidad práctica la FarmaFia y Alimentación Nutricida, y, respecto a las falsificaciones, todo el dinero que existe es falso ya que se crea de la nada. Respecto al contenido para adultos, quedan a merced de códigos morales que repriman, o no, impulsos naturales.

El 50 % restante de servicios ocultos esta dedicado a cuestiones diversas; p€olitica, anonimato, libros digitales, tecnología, juegos, ciencia, y, servicios varios (blanqueo de dinero, robos, etc.). Nada nuevo que tampoco se practique en la cupula de las PermisoCracias.

Las actividades que más predominan, redes de ordenadores zombie, y, servidores de contenidos para adultos. No obstante, si finalmente utilizáis la red Tor, y, os encontráis contenido aberrante (pornografía infantil, ofertas para realizar asesinatos, amenazas, etc.), colaborad, y, comunicadlo anónimamente a las orientadas fuerzas de seguridad institucionales.

Si queréis descubrir una nueva arma tecnológica para reducir la delincuencia sexual, consultad y apoyad el proyecto sweetie, niña virtual que persigue al infanticida depredador sexual. Actualmente, ya ha atraído y captado a mas de 100.000 usuarios que practican estos comportamientos humanamente aberrantes.

Integrantes de la red Tor recomiendan; para el envío de información, únicamente redactar archivos de texto plano evitando adjuntar archivos que puedan estar contaminados, para almacenamiento online, evitar servicios como Dropbox con evidentes fallos de vulnerabilidad, para reforzar la seguridad, conectarse a sitios con transferencia segura de datos (https), para administrar nuestra información personal en cualquier red social, permitir solo contactos de ambito personal….

Todo el contenido de este manual; Evitar Espionaje de EEUU, Proteger PC, AutoHacking, Cookies, Seguridad en Internet, Anonimato, Comunicaciones Web 100 % Seguras, etc., puede serviros para reforzar la Oferta de AutoEmpleo que elaboramos hace un tiempo, Wiki Web Way (Manual Practico para Ganar Dinero en Internet). Esta guía Abierta, Libre, y, Gratuita, va dirigida a la supervivencia monetaria en un fraudulento sistema monetario.

Además de Internetistas, y/o, Digitalistas, anunciábamos otro método de AutoEmpleo evolucionado, Monetarista. A continuación, recordamos el ultimo capitulo de la anterior guía…..

¿Y por que otro método mas de AutoEmpleo?, No os preocupéis, entre todos no ocupan mas de 2 horas al día, incluso menos. Entonces, ¿Por qué es complementario?, para estar presentes en todas las áreas que domina el inválido sistema monetario.

Las tareas de Internetista, y, Digitalista, no han sido elegidas al azar o influidas por un patrón de moda pasajero que circula por la red, atienden a causas fundamentales desconocidas por el gran público.

Hasta ahora, todos los progresos científicos y tecnológicos han sido enjaulados y aprovechados por la Corporatocracia que controla y manipula a su antojado beneficio privado "la propiedad industrial e intelectual", impidiendo así que todas sus ventajas lleguen a la gran mayoría.

La Deseconomia virtual de "libre" mercado monetario que conocéis hasta la fecha, únicamente sirve causalmente a los dueños del capital, Banco-Cleptocracia.

Ambas DES-Cracias, tan solo benefician privadamente a unos pocos a cambio de no aportar nada, se representan exclusivamente a si mismas protegiendo únicamente su tesoro mas valioso de monopolio, fabrican consumibots (usuario de bienes desinformadamente programado) orientados a sus predominantes intereses monetarios, esclavizan a la humanidad con su dinero-deuda creado de la nada, saquean los recursos territoriales falsificando nuevo dinero-deuda que crean a través del fraudulento principio de reserva fraccional, expropian cualquier patente o creación de contenido de todos los sectores productivos, etc.

¿Aun creéis que estáis en una Democracia?, la aplicación de este término no es viable ya que opera en un sistema monetario parasitario que practica la usura. Hasta la fecha, somos clientes de una DemoGracia que promueve valores distorsionados como propiedad, escasez, y competencia, en aras de ocultar las anteriores causas. Su aliado intencionadamente desinformado, la p€olitica y economi$a.

¿Podemos Liberarnos?, Si, aplicando humanitariamente la ciencia y la tecnología existente, reconociendo así la eficiencia y funcionalidad de la misma sin necesidad de nuevas leyes artificiales, códigos morales u otras programaciones sociales que las obstruyan.

Escasez, Competencia, y, Propiedad de cualquier tipo, industrial o intelectual, son tan solo mecanismos de restricción controlada que evitan la libre accesibilidad universal. No existe mayor intelecto que compartir libremente cualquier creación en beneficio de todos, para alcanzar esta meta; Abundancia Sostenible, Cooperación Global, y, Accesibilidad Universal.

El dinero, es tan solo un falso incentivo que distorsiona el autentico valor vital de los productos o servicios. La creatividad en beneficio de todos, será el autentico incentivo.

Caminando hacia estos objetivos, surgió una de las mayores fuerzas liberadoras que conecta a toda la humanidad en tiempo real distribuyendo libremente información por todas sus redes, Internet.

Obviamente, intentan controlar esta descentralizada red libre de distribución para seguir estableciendo su dominio perpetuo, y, mantener su ventaja diferencial humanamente desleal. Pero, las herramientas que nos facilita la tecnología contemporánea han creado un movimiento global que esta despertando conciencias.

La sociedad percibe que las reglas del juego son inherentemente inválidas, y, que el colapso acumulativo perpetuado por instituciones establecidas esta llegando a su fin.

Por otro lado, y golpeando desde antaño por igual a todos los demás sectores como el agrícola, manufacturero y servicios, **el desplazamiento tecnológico ha sido y es el gran causante del desempleo mundial**, y este ira en aumento si no se redirige el beneficioso crecimiento exponencial de la tecnología a favor de toda la humanidad.

Debido a esta eficacia tecnológica, expropiada por sociedades jurídicas o acciones participadas que solo sirven a los intereses del capital, el área de producción y distribución de cualquier economía no supone más del 30 %.

Si desglosamos este porcentaje, encontramos otra desproporción significante; del total de recursos monetarios destinados a esta área ProductiButiva, el 70 % va destinado a publicidad comercial, propaganda orientada.

Actualmente, cualquier corporación gasta mucho más dinero en publicidad comercial que en el proceso de elaboración del producto o servicio que distribuya.

No importa si existe o no necesidad que cubra una demanda realmente interesada, tampoco si se establecen criterios de oferta sostenible que practiquen la ausencia de desperdicio y el respeto al medio ambiente, fabricar consumibots orientados es la clave para establecer valores distorsionados y así perpetuar sus ganancias cíclicas. No importan las SocianCias.

Para realizar este lavado de cerebro, se invento una palabra muy chula, Marketing; actividad propagandística que genera entradas de pensamiento condicionado, y, produce salidas de comportamiento deseado. No interesa la Conocidad aplicada.

¿Entendéis ahora las ventajas de ser Internetista, y, Digitalista?, Ambas tareas, desde un correcto enfoque societario, cubren todas las áreas predominantes de la actual deseconomia virtual de mercado monetario. Ahora, el matrimonio entre ambos AutoEmpleos os proporcionara autosuficiencia, satisfacción, y, éxito monetario.

Como Internetistas, rastreareis las secuencias propagandísticas de productos o servicios promocionando solo aquellos que sean útiles y funcionales, es decir, priorizar la secuencia vital del valor os proporcionara frutos monetarios.

Como Digitalistas, vuestra creatividad e ingenio os permitirá desarrollar nuevos productos destinados a cualquier área ProductiButiva. La Conocidad aplicada, hará el resto.

Pero ambas actividades solo ocupan el 30 % de la actual deseconomia virtual, la siguiente evolución, Monetarista: rastreador de secuencias monetarias desde su origen hasta sus predeterminados destinos, ¿Quién se apunta?. Abstenerse predispuestos al juego sin sentido. Mantener cerca del alcance de los amigos.

El 70 % restante que completa el sistema de mercado monetario pertenece al área de finanzas e inversiones, un sector parásito que se caracteriza por no aportar nada de valor vital a la sociedad, y, que únicamente se basa en el movimiento arbitrario del dinero, tratando a este como un producto en si mismo cuando ni si quiera tiene realidad física.

Efectivamente, nos gobierna un casino, ¿Y que pasa en estos centros?, que su banca siempre gana….de momento.

En este casino, se reúnen todas las DES-Cracias; Banco-Cleptocracia, y, PlUTOcracia, ¿Y a que juegan?, a someter a su voluntad mas lucrativa a toda la humanidad, algunos llaman a este juego Democracia.

No obstante, están perdiendo la partida, la totalidad del sistema socio-económico que crearon, jerárquicamente piramidal, esta llegando a su fin, sufre daños estructurales irreparables desde su origen y fundación.

Pero, hasta que suceda el colapso del sistema monetario tras introducir el aspecto humanitario de ciencia y tecnología, jugaremos su partida.

Plantearemos varios análisis que incluyen un conjunto de métodos altamente eficaces. Sus pautas y patrones, nos ayudaran a identificar el flujo migratorio de títulos monetarios hacia destinos interesadamente determinados.

¿Alguien conoce las reglas del juego?, Ni falta, son muy sencillas, reparten las cartas hacia arriba. ¿Y como evitaremos esta trampa? Mas sencillo aun, jugando con las suyas intentando igualar la partida.

Con esta finalidad, nace *WikiBolsa*:

Enciclopedia Bursátil y Monetaria que **Informa y Comparte** Abiertamente Códigos y **Métodos** Aplicados para **Ganar Dinero** en todos los Mercados Monetarios; **Bolsa, Renta Fija, Derivados y Divisas.**

Incluye 5 Tomos:

- **"Manual Practico para Ganar Dinero en Bolsa",**
- **"€l Arte de las Perra$"**
- **"Estrategias de Inversión Caseras y Sencillas para Ganar Dinero en Bolsa y Renta Fija"**
- **"Forex Gump; El Hermano Tonto de Forrest"**
- **"Estrategias de Inversión Caseras y Sencillas para Ganar Dinero con deRRRRibados"**

Podréis disfrutar del Gratiseo durante el periodo de lanzamiento, a continuación, seguiremos las instrucciones que hemos indicado en este manual, practicar la ProductiBucion y Conocidad Funcional. Así que ya sabéis donde encontrarnos.

Quedara a vuestra disposición compartir el contenido de esta Libre Enciclopedia como Afiliados, siempre y cuando os parezca apropiado.

En los manuales 3 y 5, optaremos únicamente por la anterior estrategia, ofreceremos un 75 % de las ventas realizadas, ¿Por qué motivo?, Para que podáis destinar las SocianCias al AutoEmpleo de Monetarista. De nuevo, prevalecen las SocianZas.

Desde la Plataforma y Extensión online que hemos creado, www.wikibolsa.org, podréis todos los Usuarios: Participar activamente, Consultar cualquier Estrategia Publicada, Acceder a video-Tutoriales, Contribuir de modo Escalable Mejorando todo el contenido, Descubrir un programa de soluciones para superar todas las crisis, Intercambiar información relevante, etc...

InterneTistas, y/o, Digitalistas, si también queréis formaros como Monetaristas, os estamos esperando…

¿Habéis aprendido, y, disfrutado de una experiencia vital, satisfactoria, estimulante, constructiva, amigable, interactiva, funcional, etc.?

Si la afirmación a la cuestión ha sucedido, esperamos vuestra colaboración de expansión masiva: Copiad, Prestad, Modificar, Redistribuir, Divulgar, y, Compartir este Manual Practico de Liberalización Informática Socialmente Satisfactorio.