Linux, seguro y fácil

por Lorenzo Peña

····· 2004-04-27 ·····

Índice

La argumentación que ofrezco en este artículo, complementaria de la de ensayos anteriores, se va a dirigir sólo a dos factores: la seguridad y la facilidad. Muestro que son erróneas e infundadas las alegaciones de que el sistema Linux es inseguro y difícil.

§1.— Seguridad

Las revistas linuxeras vienen consagrando artículos al tema de la seguridad. Mis consideraciones no reemplazan esos desarrollos más profundos y documentados de los expertos, sino que son el fruto de la reflexión de un no profesional.

Conviene, ante todo, aclarar qué es seguridad. Seguro es lo opuesto a inseguro; e inseguro es lo que conlleva riesgo o peligro. El peligro lo es siempre de algo malo, y consiste en una probabilidad, mayor o menor, de que suceda ese algo malo.

Tal probabilidad puede ser objetiva o subjetiva. La objetiva estriba en algún tipo de propensión real (independiente de las expectativas, las esperanzas o los temores que podamos albergar). Una manera de entender esa propensión es haciéndola consistir en frecuencia; mas la frecuencia y la infrecuencia suponen algún término relativo. Puede ser frecuente tener ojos azules entre los escandinavos pero infrecuente, o menos frecuente, entre los habitantes de tal barrio de Copenhague.

La inseguridad subjetiva es un temor razonable a que suceda el hecho malo que no se desea.

Muchas veces se mezclan las nociones de inseguridad subjetiva y objetiva, lo cual es disculpable bajo ciertos supuestos de información y de racionalidad, que no siempre se cumplen. En ausencia de información adecuada o de buena capacidad razonadora, puede coexistir alta inseguridad objetiva con una (infundada) confianza subjetiva; y puede darse un alto temor de un suceso que objetivamente tenga escasas posibilidades de realizarse.

Por otro lado, la seguridad objetiva, o ausencia (relativa) de riesgo, puede ser directa o indirecta. La directa se da cuando es pequeño o nulo el peligro en cuestión, e.d. cuando de hecho hay escasas posibilidades de que suceda (la propensión o tendencia a tal suceso es escasamente verdadera o real).

La indirecta es la probabilidad de que, de suceder el evento temido, se alivien o se remedien sus nocivos efectos por algún medio previsto.

La prevención de los riesgos (o sea la securización objetiva) consistirá, si es directa, en impedir que acaezcan, o sea: en causar un incremento de la probabilidad objetiva de que no acontezcan; al paso que la prevención indirecta, o impropia, consistirá en estar precavidos para el infortunio a fin de evitar su plena consumación, o al menos limitar sus efectos o compensarlos.

Cuando contratemos una póliza de seguros, o cuando estemos protegidos por la seguridad social (inicialmente llamada 'previsión social') —ya sea seguro de vejez, de enfermedad, de desempleo etc—, aquello de lo que disfrutaremos será sólo una garantía de que, de producirse el evento temido, obtendremos un remedio para atajarlo, hacerle frente o aliviar sus consecuencias causales.

(Si hubiera de veras medicina preventiva, estaríamos en una securización directa; no la hay —como tampoco hay política pública encaminada a evitar el desempleo, que sería otro medio para proporcionar seguridad directa.)

Hay riesgos específicos que son los que se corren con el manejo de sistemas electrónicos e informáticos, y concretamente de sistemas operativos (junto con el *software* que, sin formar parte en rigor de tales sistemas, viene incorporado y asociado a ellos —cual sucede, p.ej., con el programa de procesamiento de texto MicroSoft Word, con el visualizador Internet Explorer y con el programa de correo electrónico Outlook, estrechamente unidos los tres al sistema operativo Windows).

Tres de esos principales riesgos son:

(1) La involuntaria ejecución de programas malignos (genérica, aunque sea impropiamente, conocidos como 'virus electrónicos');

(2) La penetración ajena en nuestra máquina al estar conectada con el internet (allanamiento electrónico); suele ser un ataque a una máquina conectada por ADSL o cable-modem, pudiendo acarrear otras consecuencias, como la abusiva utilización de nuestros recursos por el intruso, la averiguación de secretos y la ejecución, sin consentimiento del dueño, de programas que propaguen spam o virus;

(3) El mal funcionamiento de programas en sí benignos, con resultado de desperfectos, averías, interrupciones (cuelgues) y hasta borramiento de ficheros (pérdida de datos).

Sentadas esas precisiones, hay que decir que un motivo por el que Linux no sólo ha venido recomendado entre el público sino que se ha ganado la aceptación de muchos usuarios competentes y serios es que este sistema operativo es objetivamente más seguro que el Windows en cualquiera de sus versiones, o, como mínimo, muchísimo más que las versiones populares del Windows.

Y, siendo objetivamente más seguro, provoca también en los usuarios una actitud de serena confianza, una grata sensación de estar al abrigo de los disgustos, lo cual hace más satisfactorio el trabajo electrónico. Este factor de la mayor seguridad subjetiva es, sin duda, de menor importancia, mas no cabe olvidar que, si las computadoras han mejorado nuestra calidad de vida (al allanar la realización de una serie de tareas),

también pueden generar un cierto deterioro de esa calidad de vida, al acarrear turbación y desencanto, ya que, en el ámbito informático, a menudo las cosas no ocurren como se esperaba.

Desde luego, aunque es valiosa la tranquilidad de ánimo, por sí sola, no es muy deseable obtenerla por ignorancia; un usuario ingenuo del Windows, que viva en candorosa inocencia, puede que experimente una serenidad paradisíaca, que le envidiamos, aunque quizá preferimos, habida cuenta de todo, ser conscientes de los peligros.

Está siendo cuestionada últimamente la tesis de la superioridad del Linux en lo tocante a las condiciones de seguridad que proporciona, no sólo por la casa Microsoft y sus adeptos y colaboradores, sino también por periodistas informáticos presuntamente independientes y por algunas firmas de consultoría electrónica e informática, las cuales han difundido varios informes en los que, compilando y utilizando estadísticas, se alcanzan conclusiones sorprendentes al respecto.

Es más, el dogma de la superioridad del Linux en este punto viene en parte quebrantado —o más exactamente matizado— incluso por ciertos partidarios del Linux, quienes aducen que el Linux también tiene problemas propios de seguridad, y que, si bien es en eso mejor que el Windows, la excesiva confianza en su superioridad conduce a un rebajar la guardia que acaba haciendo al sistema mucho menos seguro de lo que se creía.

A esas alegaciones y a esos escrúpulos respondo con las consideraciones que siguen.

1º) Hay un adagio filosófico de que *contra facta non sunt argumenta*; contra los hechos no valen los argumentos. Y es un hecho que el usuario del Linux está casi siempre a salvo de los atentados a la seguridad que sufren muchísimos usuarios del Windows —quizá la mayoría de ellos; el principal de esos atentados es la infección por virus que se sufre al recibirse en el programa de email Outlook un mensaje infectado (al margen de averiguar por qué mecanismos se contagia la infección). Esa diferencia de riesgo puede medirse de diversos modos: uno de ellos es la frecuencia del padecimiento de tales quebrantos (proporción de usuarios del sistema operativo afectados frente a los no afectados). Explíquese como se explique, es mayor para un usuario medio de Windows que para uno de Linux la posibilidad de sufrir percances indeseados.

2º) Además, hay tres explicaciones simples de esa disparidad de riesgo que tienen que ver, no con el grado de pericia y de cultura de los respectivos usuarios, sino con estos tres principios:

[1ª] **Principio de publicidad** o transparencia: el Linux es un sistema de fuente abierta, lo que significa que los programas incorporados al sistema operativo (no forzosamente todos los que corran bajo ese sistema operativo) tienen, públicamente accesibles, los códigos, los textos de las instrucciones redactadas en un lenguaje de programación. Es, como si dijéramos, que no sólo podemos escuchar una ejecución musical, sino también leer la partitura. Al estar públicamente

accesibles esas fuentes, los errores que den lugar a riesgos para la seguridad pueden ser detectados por cualquiera (de los miles y miles de programadores que forman parte del público) y, una vez denunciados, habrán de ser prontamente corregidos por los autores de los programas (salvo que a éstos no se les dé un ardite en quedar desacreditados). En suma, se trabaja en un ambiente de pública y mutua inspección, de franco control recíproco, de cooperación similar a la que rige en la comunidad científica.

En cambio con sistemas operativos de fuente oculta eso no es posible. Sólo la casa dueña del software puede, si lo juzga oportuno, corregir el programa y taponar las brechas. El público a lo sumo puede percatarse de los resultados de los fallos, aunque diagnosticar la causa siempre es tan problemático aquí como lo es en medicina. Si fuera públicamente accesible el código de nuestra anatomía y fisiología, sería mucho más fácil prever enfermedades y prevenirlas, así como diagnosticar las que se produzcan.

[2ª] **Principio de parsimonia** (o de minimalidad), consistente en no ejecutar una tarea más que cuando explícitamente haya expresado el usuario el deseo de realizarla; o, en otros términos, que está prohibido que se ejecute lo que el usuario no ha permitido expresamente.

En Windows —y en general en los sistemas dizque amigables— rige el principio opuesto, el de exuberancia o maximalidad: en aras de suavizar al máximo las tareas, los diseñadores del sistema —al que ellos reputan amigable— deciden efectuarlas de oficio, o sea: dárselas consumadas al usuario sin que éste lo pida, en virtud de una presunción contextual de que el usuario desearía tal ejecución.

Así, p.ej., el MSWord, al recuperar un documento, ejecuta las macros incorporadas al documento (guiones, *scripts*); y, al guardarlo, incrusta en él macros; las macros son microprogramas ejecutables, que efectivamente vienen ejecutados por el Word. Cuando el usuario cree estar meramente recuperando un texto para leerlo o imprimirlo, está dando lugar a que, sin consultarlo, el Word ejecute las macros anejas al texto en cuestión; eso para ahorrarle al usuario el esfuerzo de decidir si quiere o no que se ejecute tal o cual macro, que podría afectar a la presentación del documento (y así se evita que haya separación de forma y de contenido: el usuario nunca trabajará con un texto mondo y lirondo, sino siempre con uno formateado de determinada manera, como lo haría si escribiera a máquina; un eventual reformateo es posible, pero difícil).

Igualmente se comportan el Outlook, el Explorer etc. Todos ellos, en aras de dárselo todo mascado al usuario, llevan a cabo tareas que —se supone— él desea se realicen, sin haberlo solicitado para nada.

Aunque puede que haya en Linux programas que, en parte, se inspiren en esa visión de las cosas (tal vez algunos programas en modo gráfico), en general la concepción linuxera es opuesta: sólo se ejecuta lo que el usuario decide ejecutar: al abrirse un texto, éste se despliega sin que se ejecute macro alguna; al abrirse un mensaje de email, no se ejecuta ningún programa que

pudiera a su vez pasar el control a macros incrustadas o infiltradas en el mensaje; si el usuario desea, puede guardar el mensaje y, desde fuera, o luego, ejecutar otros programas (de audición, despliegue gráfico, acceso a internet, etc), aunque incluso en ese caso los programas linuxeros probablemente no aceptarán ejecutar macros agazapadas.

Ese método es menos amigable que el del Windows, pero mucho más seguro. Fuerza al usuario a tomar ciertas decisiones, mas le ahorra los efectos nocivos de decisiones ajenas.

[3ª] **Principio de compartimentación**: el sistema de permisos del Linux limita los daños. Tal vez alguna de las últimas versiones del Windows esté (¡por fin!) introduciendo algún sistema similar; pero, hasta donde he podido observar, no así las versiones hasta ahora populares.

El sistema de permisos del Linux sería mejorable, habiendo ya distribuciones (y versiones del kernel) que lo refinan y refuerzan. Tal como está, sin embargo, es sumamente útil. Ese sistema hace que los ficheros y directorios de los que es dueño (*owner*) un usuario no sean accesibles para otros (o que sólo lo sean limitadamente para un grupo determinado de usuarios, si así lo decide el propio usuario en cuestión).

En sentido técnico, un **usuario** no es un individuo sino un papel —o un rol— caracterizado por un nombre (*username*) exclusivo. Un mismo individuo puede acceder a su máquina —alternativa o hasta simultáneamente— con roles (y *usernames*) distintos, mientras que varios individuos pueden compartir un *username* y emplearlo alternativamente, uno u otro. (En este último caso —para decirlo paradójicamente— varios individuos son un solo y mismo usuario.)

En cualquier sistema UNIX, incluido el Linux, hay un rol privilegiado, un superusuario, el *root* o administrador del sistema. Los ficheros de los que él es dueño no son, en principio, reescribibles ni borrables por ningún otro usuario. El individuo que juega el papel de *root* puede (y debe) usar otros roles con sendos *usernames*; al entrar en la máquina con esos otros roles, no puede borrar los ficheros de los que es dueño el *root*.

Con un poco de astucia, ese mecanismo permite a un mismo usuario real desdoblarse en varios usuarios virtuales (roles), a diversos efectos (lo que le impone tener que acceder con sendas contraseñas, aunque hay atajos), impidiendo que, por error o aturdimiento, pueda él mismo estropear en una sesión sus ficheros pertenecientes a otro ámbito, a los que accede en otra sesión (pudiendo abrirse pasarelas).

Es verdad que ese sistema de permisos sólo sirve de algo si el usuario hace caso a los consejos —que se le prodigan en toda la documentación linuxera— de servirse de él. Si se empeña en activar sólo el rol de *root* y en hacerlo todo sólo siempre como ese único usuario, *root*, entonces el sistema no le habrá valido de nada.

3º) Esos tres principios precautorios suelen evitar las catástrofes o limitarlas, pero también sirven para, llegado el caso, remediarlas (seguridad indirecta, en la terminología de más arriba).

Así, la publicidad de las fuentes puede determinar que, si un programa, por ciertos fallos, causa algún desperfecto o una pérdida de datos, será fácil que se anuncien públicamente no sólo medios para evitar el daño en el futuro, sino también vías para resarcirse del daño ya producido (al saberse cómo se ha originado).

Igualmente, la regla de ejecución mínima o parsimoniosa permite que, si el usuario, por imprudencia, comete un error funesto, se atenúen las consecuencias, y sean más fáciles de reparar que si se desencadenara una cadena de resultados que él no haya previsto.

Y también el sistema de permisos facilita remediar los daños, mediante previos respaldos compartimentados, al paso que el tropel del proindiviso ventanero puede hacer inviable la recuperación.

4º) Frente a tales consideraciones, los adeptos de Microsoft aducen varias objeciones.

[1ª] Una es que muchos ojos no ven más que pocos, porque lo que cuenta es la calidad, no la cantidad. Los programadores de MS son mejores, trabajan en equipo, ordenadamente, al paso que la dispersa muchedumbre de informáticos linuxeros son a menudo diletantes, y actúan sin orden ni concierto. Lo que contaría en esto sería la profesionalidad que sólo puede brindar una empresa responsable, nunca la multiplicación de los opinantes y arbitristas.

[Respuesta] La concertación y el plan son necesarios, o al menos convenientes, para elaborar algo, sea un programa o cualquier otra cosa. Mas esa concertación no requiere hacerse con ánimo de lucro, siendo ese ánimo el que diferencia a las empresas de otras personas individuales o colectivas. La planeación, la ordenación de esfuerzos, pueden darse y se dan también en asociaciones desinteresadas, centros académicos de investigación, etc. Y cualquier individuo es capaz de actuar también según un plan y no al buen tuntún. También la responsabilidad puede ser asumida igual de bien por un colectivo sin ánimo de lucro que por una empresa.

Mas, para enjuiciar una obra, para hallar sus fallos y someterla a la crítica, para sugerir mejoras, es preferible la multitud, la mayor pluralidad, sin que sea menester (ni siquiera bueno) que haya concertación entre los críticos.

[2ª] La difusión de las fuentes permite también a programadores malignos introducir disfunciones deliberadas, y luego propagarlas, al paso que el secreto de esas fuentes, si está bien guardado, pone a salvo al usuario, gracias a la seriedad y responsabilidad de la casa productora del *software*, la cual tiene interés en la calidad y buen funcionamiento de

sus productos, que son las mercancías que vende, ya que sólo así mantendrá la confianza de sus clientes.

[Respuestas]

[Primera] En primer lugar, el usuario tiene pocos motivos para presumir la buena fe de esas casas monopolísticas. Carece de elementos de juicio, porque es un enigma, o un secreto comercial, qué pasa en ellas, de puertas adentro. Sólo puede hacer la inferencia a la que lo invitan los monopolizadores a saber: «¡Confíe en que somos honestos porque, si no lo fuéramos, Ud se acabaría dando cuenta y dejaría de confiar en nosotros!». Un razonamiento de un valor muy relativo y al cual podría recurrir cualquiera con alguna posición de dominación o hegemonía. Mas, aunque sea válido, no hay más motivos para presumir la buena fe de una casa comercial monopolística que la de asociaciones, entidades o páginas *web* reputadas, consolidadas, que se han ganado a pulso la confianza de miles de usuarios inteligentes y con conocimiento de causa, las cuales se encargan de ofrecer gratuitamente distribuciones del Linux y programas de fuente abierta que corren bajo Linux, así como, eventualmente, actualizaciones, parches, correctivos y mejoras, cuando además la actuación de esas entidades es transparente, no guareciéndose en el secreto comercial.

[Segunda] Hay motivos para sospechar la mala fe de los monopolizadores en algún aspecto; p.ej. que introduzcan en nuestra máquina chivatos u otros programas agazapados (para alertar a la casa comercial de la eventual copia indebida o del uso de un *software* rival), los cuales pueden ser explotados por terceros desaprensivos para usos aún más perjudiciales (para infiltrarse en nuestra máquina y hacer *spam* desde ella, u otras cosas peores).

[Tercera] Al margen de la buena o mala fe, ofrecer un producto seguro es una cuestión de eficacia. Habrá de ser apreciado por cada uno según su experiencia el grado de eficacia de la empresa monopolística de que hablamos (MicroSoft). En general los monopolios pueden a menudo conducir a ineficiencias; en este punto, hay motivos concretos para ser sospechar esa ineficiencia. Sin cuestionar la buena voluntad de los jefes, su deseo de ofrecer al público una mercancía informática de calidad y segura, lo que constatamos es que no lo han logrado, según lo prueba la espantosa inundación de virus, *spam* y viruspam que ha anegado al mundo de los usuarios del Windows (principalmente a través del desdichado Outlook), derramando y proyectando ese *spam* también hacia los usuarios del Linux (aunque para éstos el único efecto nocivo sea la saturación de sus buzones de email).

[Cuarta] El principal motivo de inseguridad informática no consiste en que el programa que uno adquiere haga de las suyas (aunque eso también sucede, como cuando el Windows cuelga la máquina cada dos por tres

o se obstina en rehusar nuevo *hardware* sin desinstalar el soporte del previamente incorporado). El principal problema es que los programas pueden ser aprovechados por terceros para, sobreañadiendo ciertos módulos o infiltrando macros, causar destrozos o efectos indeseables (p.ej. la temida propagación de *spam*). Y para aprovecharse de programas de elaboración ajena insertando tales cuñas maléficas no es menester leer las fuentes. Lo prueba la horrorosa proliferación de virus, *spam* y viruspam que aqueja a muchas de las máquinas que corren bajo Windows, cuando presumiblemente los malignos inventores de todo ese cúmulo de cuñas ignoran las fuentes de Microsoft, pero se percatan de los fallos en el funcionamiento real de los programas de Microsoft, sobre todo en el Outlook.

[3ª] El sistema de permisos no preserva los datos de un usuario al que se le infiltren virus (que son posibles también en Linux); sólo salvaguarda a los ficheros del *root*, que frecuentemente son los de menos valor, porque suelen ser sencillamente los programas instalados, que se reinstalan desde CDRom (o medio similar).

[Respuesta] Si se usa con un poco de inteligencia —o simplemente de astucia—, el sistema de permisos pone los datos de un usuario virtual a salvo incluso de la negligencia o del infortunio de otro usuario virtual, aunque sean ambos el mismo individuo real de carne y hueso. Puede Ud abrir su email como usuario ‘anamari’ y sus textos como usuario ‘remedios’, estableciendo —con precaución— pasarelas de uno a otro usuario. Aunque no conozco a ningún usuario del Linux al que se le hayan introducido virus (virus para Linux) que le hayan hecho perder datos, podría suceder, claro, y acabará sucediendo algún día. Suceda o no, uno puede cometer un error, borrando lo que no querría borrar. Ese desdoblamiento limita los daños, poniéndolo a uno a salvo de sus propios descuidos; comprendo que alguien puede juzgar engorroso ese desdoblamiento en varios usuarios; si se acostumbra a hacerlo, le resultará una rutina liviana, cuya práctica lo pondrá a salvo de peligros (principalmente, en realidad, del peligro de borramientos por alguna precipitación o imprudencia propias).

[4ª] Según ciertos informes de determinadas firmas de consultoría electrónica, ha habido, en ciertos períodos de tiempo recientes, más irrupciones en máquinas con Linux que con Windows. De hecho han sido agredidas y desfiguradas varias páginas *web* emblemáticas de algunas tribunas del Linux; es posible que sea atacado un sitio Linux, por alta que sea su reputación, y que un usuario cualquiera acceda en ese momento, se baje programas adulterados sin saberlo, y se produzca una catástrofe en su máquina, incluso la pérdida de datos.

[Respuestas]

[Primera] Hay que comparar lo comparable. Aun aceptando la honradez e imparcialidad de esas consultorías, lo que el autor de estas líneas ha podido percibir es que esos dizque estudios no comparan cosas comparables. Hay muchas páginas *web* de aficionados, caseras, experimentales, que son llevadas por muchachos que se han entusiasmado por el Linux o, sencillamente, que han descubierto la potencia de ese sistema operativo, sin ser expertos o sin ser avezados. Hay, al parecer, pocas páginas así llevadas bajo el Windows. Es normal que se vea arrollado el *webmaster* incauto y diletante, que ni siquiera ha instalado un cortafuegos (*firewall*). Lo que habría que ver es si, con relación al mismo género de situación (al mismo grado de profesionalidad, dedicación y capacitación técnica), hay más asaltos con éxito en Linux; y eso no parecen decirlo los pseudoestudios citados. Dudo que haya estadísticas, pero parece fundada la impresión justamente opuesta.

[Segunda] En cuanto a la credibilidad de los estudios, desgraciadamente no siempre están claros los datos, criterios y métodos utilizados. Peor que eso es que difícilmente puede presumirse la inocencia de los consultores, cuando a veces están, directa o indirectamente, vinculados por lazos de negocios con la casa Microsoft. Digamos, en el mejor de los casos, que los ciega el interés de sus amigos y socios, aunque crean ser objetivos y hasta se afanen infructuosamente por serlo. Su subconsciente los traiciona. Se han hecho tantas alegaciones al respecto que, sin medios ni ganas para comprobar nada de todo eso, prefiero abstenerme de emitir juicio alguno y otorgarles el beneficio de la duda.

[Tercera] ¿Hay peligro de bajarse programas de una página *web* del Linux previamente corrompida por un malévolo intruso? Las posibilidades parecen próximas a cero. Aunque se materializaran, la publicidad que rige la vida del Linux remediaría rápidamente el problema y pondría al usuario a salvo de daños, salvo si incurre en extrema precipitación. Hasta donde sé, todo eso son meras especulaciones.

En conclusión, creo que son endebles e infundadas las objeciones de los adeptos del monopolio ventanero. El sistema operativo Linux es seguro, aunque desde luego su grado de seguridad no es del 100%. El usuario terminal que otorgue un alto valor a la seguridad hará bien en optar por Linux.

§2.— Facilidad

Si el Linux es seguro, también es —se nos dice— difícil, al paso que el Windows es fácil y cómodo.

De nuevo hay que comparar lo comparable. Es más difícil hacer en Linux cosas difíciles que en Windows cosas fáciles. Eso es verdad.

También es verdad que a quien está acostumbrado al Windows le resulta fácil seguir con el Windows. La facilidad es relativa. Un idioma no es más fácil que otro

salvo para el hablante que lo usa habitualmente o con relación a un tercer idioma (según el parecido respectivo). Y, si bien un sistema operativo no es un idioma, ni su facilidad o dificultad son las de un idioma, el símil no es del todo infundado, porque el manejo de unos procedimientos informáticos u otros tiene algo de similar al manejo lingüístico, al empleo de un sistema de señales.

Para determinar si el sistema Linux es fácil, o cuán fácil es, hay que medir tanto el tiempo de aprendizaje cuanto el grado de eficiencia que se alcanza con una determinada inversión de ese tiempo de aprendizaje.

La comparación se resolvería inmediatamente si fuera cierto que el Windows se maneja con un tiempo de aprendizaje cero, cual nos lo presentan sus adeptos. La experiencia de quien esto escribe desde luego desmiente tajantemente ese alegato, que no pasa de ser un mito. Con un aprendizaje cero no sólo no se da pie con bola (es improbable que salga nada bien, ni aun por casualidad), sino que se pueden provocar catástrofes en el entorno ventanero.

Lo que sucede es que hay más personas que manejan Windows, y esas personas pueden transmitir su sabiduría a otros. Si alguien le enseña cómo abrir el Outlook, cómo manejar un poco el Word, cómo moverse mínimamente en el Explorer, y le dan a Ud, ya instalado desde la tienda, el sistema operativo, eso es más fácil que instalarse uno Ud mismo o aprender el manejo en una documentación, cuando no conoce personalmente a ningún linuxero.

Windows deja de ser fácil cuando sucede algo; algo como que Ud compra un dispositivo adicional (porque, aunque tal vez Windows lo va a reconocer en seguida, puede provocarse un conflicto con dispositivos preinstalados, hasta el punto de tener que reinstalarlo todo desde cero); algo como que se corrompa algún fichero de configuración y haya que entrar «a modo de pruebas», sintiéndose uno vendido y desamparado; algo como tener que hacer frente a quebrantos de seguridad (considerados en el apartado §1 de este ensayo).

En todos esos casos, y en muchos otros imprevistos, se desvanece la facilidad, sin que Windows haya ofrecido al usuario normal una capacitación para hacer frente a tales situaciones (y sin que la garantía de Microsoft sirva a esas alturas de nada).

Por otro lado, muchos usuarios emplean los programas informáticos para un elenco reducido de tareas, como escribir pequeños documentos (cartas, cortos artículos, esquemas, etiquetas, páginas *web*), manejar el correo electrónico, bajarse ficheros musicales, comprimirlos o descomprimirlos (MP3), grabar CDs, importar ficheros PDF, imprimir, llevar una agenda, hacer cálculos o cuentas, manejar algunos gráficos, volcar fotos, etc.

Para tales tareas hay programas de sobra en el Linux que realizan todo eso adecuadamente y sin gran dificultad. Puede resultarle difícil a alguien aprender cómo usarlos si está acostumbrado a los del Windows —aunque la dificultad tiende a ser pequeña, por la inclinación actual de los distribuidores del Linux a imitar al Windows más allá de lo razonable.

Es más, muchas de esas tareas sencillas se pueden llevar a cabo incluso con programas del viejo DOS, programas que se pueden ejecutar bajo Linux muy fácilmente corriendo el programa dosemu —un emulador del DOS.

Así, están programas como el insuperable WordPerfect 5.1, con el cual se pueden escribir y mantener libros, ficheros, acervos de datos (ficheros de fusión), se pueden hacer clasificaciones, se pueden usar notaciones simbólicas, esquemas, estilos, tipos de letra, revelar códigos. Hay otros programas para DOS que permiten hacer casi todas las tareas recién mencionadas, y que corren muy bien bajo Linux (a través del dosemu). El manejo de esos programas es fácil, sencillo, claro, rápido, prescindiendo de adornos y de distracciones.

También es relativamente fácil en Linux llevar a cabo conversiones de unos formatos a otros (o, por lo menos, es, al parecer, más fácil que en Windows).

Los programas ventaneros suelen ser lentos, pesados, opacos, abusando del método *wysiwyg* (*what you see is what you get*, o sea revoltijo de forma y contenido, que hace muy difícil el reformateo).

Es más fácil en Linux que en Windows hacer una tarea rápidamente, hacerla bien, convertir, reformatear, reconfigurar el uso de los programas, almacenar los resultados en menos espacio de disco.

Es más fácil en Linux que en Windows usar viejo *hardware*: viejas impresoras, discos duros de escasa capacidad de almacenamiento, tarjetas ethernet desfasadas, máquinas de segunda mano.

Es más fácil en Linux que en Windows cargar, según los casos, unos u otros módulos (p.ej. tener un disco duro introducible de quita y pon, arrancando unas veces de un modo y otras de otro modo).

Es más fácil en Linux que en Windows entender el uso de los programas, si uno quiere adentrarse en el manejo solvente y rebasar la condición de párvulo. Son de escaso socorro las ayudicas en línea, apenas visibles (salvo para personas con gran acuidad visual), al paso que los manuales del Linux están bien redactados y suelen disipar todas las dudas.

También es más difícil en Windows que en Linux instalar convenientemente los programas y disponer de opciones de instalación flexibles. Las instalaciones de programas ventaneros suelen ser rígidas. Es más, en ese entorno se suelen escondenrincluso las pocas opciones de instalación fructíferas e interesantes que, sin embargo, están en teoría disponibles, como p.ej. las de conversión (por lo cual tantos usuarios del Word serán incapaces de leer documentos que les enviemos en formatos diferentes del *.doc*, el *.rtf* u otros así).

También es más difícil en Windows que en Linux librarse de los incordios, las molestias, los acosos para actualizar los programas, registrarse, importar parches disponibles, confesarse con los dueños del *software* y rendirles homenaje y tributo.

También es más difícil en Windows que en Linux prescindir de los procesos tediosos y lentos de reinstalación, o acelerarlos, evitando tener que rearrancar la máquina

ochenta veces con cada nuevo programa, o con cada nuevo adminículo o periférico adicional.

También es más difícil en Windows que en Linux entenderse con quienes usan otro sistema operativo y otros programas. A cambio es más fácil entenderse y comunicarse con quienes usan Windows (más el Outlook, el Word, el Explorer etc).

A juzgar por la experiencia, también es probablemente más difícil en Windows que en Linux producir documentos en PDF, enviar a la impresora ficheros desde el intérprete de órdenes, usar disquetes o CDs de formatos no estándar, hacer conversiones, compilar programas, abrir particiones de otros sistemas operativos, lanzar consolas DOS paralelas con diferente configuración, y en general realizar cualquier tarea a la que no hayan prestado mayor atención los diseñadores del entorno gráfico.

También es más difícil en Windows que en Linux intercambiar discos duros, arrancar desde diversas particiones (con versiones a prueba del sistema operativo, o de otros sistemas), y en suma experimentar alternativas.

Para cerrar este apartado, voy a referirme someramente a las tribulaciones de uno que quiso reinstalar una versión del Windows después de haberla adquirido preinstalada y haberla borrado (para reformatear el disco duro).

El Windows rechazó reinstalarse; celosamente declinó compartir el disco duro particionado con otros sistemas operativos; se negó a usar CDs de instalación, aduciendo que eran sólo de actualización, siendo requisito necesario tener ya preinstalada una versión anterior; al intentar el usuario —para solventar esa dificultad— instalar primero el viejo Windows 95 (para luego «actualizarlo» o ascenderlo a otro Windows más reciente), fue imposible, por no venir reconocido el *hardware* moderno por el Windows 95.

El testarudo usuario a quien me estoy refiriendo acabó hallando un truco, a través del Linux, gracias al cual pudo volcar el Windows de una máquina a otra (al precio de afrontar luego un amargo día de rearranques y reconfiguraciones, que habrían agotado la paciencia del Santo Job, y por el cual espera alcanzar indulgencia plenaria a la hora de entrar en el Purgatorio).

Como ejercicio mental, o como prueba de obstinación, puede ser interesante. Desde luego es cualquier cosa menos fácil.

En suma, el Windows es más fácil en unas cosas, y sobre todo para quienes están acostumbrados a él y se ajustan a las predeterminaciones estándar. Es más difícil en y para muchas otras cosas.

Dado todo eso, ¿cómo entender que incluso un número de linuxeros piensen y digan que Linux no es para papá y mamá? Tal vez lleven razón, si a papá y a mamá se les da puesta una computadora con Windows y se les ofrece como alternativa un CD para que se instalen Linux. A papá y mamá, o a cualquiera. Pero, si se compara lo comparable, ese alegato no le resulta nada verosímil a quien esto escribe. Para manejar Linux no es menester ser un informático ni haber aprendido lenguajes de programación, ni ser un experto. Y, como hemos visto, si papá y mamá se ven en el trance de querer emprender ciertas tareas, puede resultarles más difícil hacerlas con Windows.

La leyenda de la dificultad del Linux no se despejará con argumentos como el aquí expuesto. Igual que otras leyendas negras, viene propagada por quienes tienen interés en que se mantenga tenazmente arraigada. Pero sabemos que algunas leyendas así acaban perdiendo crédito, porque el intelecto humano se revela más fuerte que los prejuicios.

Conclusión

Hemos considerado dos cualidades: seguridad y facilidad. En la primera triunfa el Linux. En la segunda, hay bastante margen para la duda, y tal vez todo dependa de la perspectiva; acaso en cuanto a facilidad, el orden no sea lineal (e.d. ni sea, así a secas, más fácil el Windows ni lo sea el Linux, sino que en unas cosas lo será el uno y en otras el otro).

Pero el Linux es seguro y es fácil, mucho más fácil de como lo pintan.